


[Help](#)
[Logout](#)
[Interrupt](#)
[Main Menu](#)
[Search Form](#)
[Posting Counts](#)
[Show S Numbers](#)
[Edit S Numbers](#)
[Preferences](#)

## Search Results -

Terms	Documents
l4 and @fd<=19990327	0

☐ US Patents Full-Text Database  
☐ US Pre-Grant Publication Full-Text Database  
☐ JPO Abstracts Database  
☐ EPO Abstracts Database  
☐ Derwent World Patents Index  
☐ IBM Technical Disclosure Bulletins

Database:

Refine Search:

## Search History

Today's Date: 12/5/2001

DB Name	Query	Hit Count	Set Name
USPT	l4 and @fd<=19990327	0	L5
USPT	(drm\$ or (digital adj right adj management) or (digital-right-management)).clm.	25	L4
USPT,PGPB,JPAB,EPAB,DWPI,TDBD	l1 and l2	4	L3
USPT,PGPB,JPAB,EPAB,DWPI,TDBD	(drm\$ or (digital adj right adj management) or (digital-right-management))	1104	L2
USPT	((705/51  705/59  705/57 )!.CCLS. )	408	L1

*reviewed* →  
 No "hit" in NPL database  
 "Dialog"

**WEST**[Help](#)[Logout](#)[Interrupt](#)[Main Menu](#)[Search Form](#)[Posting Counts](#)[Show S Numbers](#)[Edit S Numbers](#)[Preferences](#)

Your wildcard search against 2000 terms has yielded the results below

Search for additional matches among the next 2000 terms

starting with: WEB\$(WEBER-CO-INC-H-G).P23-P27,P20-P22,P1-P18.

**Search Results -**

Terms	Documents
(drm\$ or (digital adj right\$1 adj management) or (digital-right\$1-management)) and ((digital adj license) and (network\$ or Internet or web\$))	4

US Patents Full-Text Database  
US Pre-Grant Publication Full-Text Database  
JPO Abstracts Database  
EPO Abstracts Database  
Derwent World Patents Index

Database: IBM Technical Disclosure Bulletins

Refine Search:

(drm\$ or (digital adj right\$1 adj  
management) or  
(digital-right\$1-management)) and

Clear

**Search History**

Today's Date: 12/5/2001

<u>DB Name</u>	<u>Query</u>	<u>Hit Count</u>	<u>Set Name</u>
JPAB,EPAB,DWPI	(drm\$ or (digital adj right\$1 adj management) or (digital-right\$1-management)) and ((digital adj license) and (network\$ or Internet or web\$))	4	<u>L7</u>
JPAB,EPAB,DWPI	I2	300	<u>L6</u>
USPT	I4 and @fd<=19990327	0	<u>L5</u>
USPT	(drm\$ or (digital adj right adj management) or (digital-right-management)).clm.	25	<u>L4</u>
USPT,PGPB,JPAB,EPAB,DWPI,TDBD	I1 and I2	4	<u>L3</u>
USPT,PGPB,JPAB,EPAB,DWPI,TDBD	(drm\$ or (digital adj right adj management) or (digital-right-management))	1104	<u>L2</u>
USPT	((705/51  705/59  705/57 )!.CCLS. )	408	<u>L1</u>

**WEST**☐ Generate Collection

L3: Entry 3 of 4

File: USPT

May 29, 2001

US-PAT-NO: 6237786

DOCUMENT-IDENTIFIER: US 6237786 B1

TITLE: Systems and methods for secure transaction management and electronic rights protection

DATE-ISSUED: May 29, 2001

## INVENTOR-INFORMATION:

NAME	CITY	STATE	ZIP CODE	COUNTRY
Ginter; Karl L.	Beltsville	MD		
Shear; Victor H.	Bethesda	MD		
Spahn; Francis J.	El Cerrito	CA		
Van Wie; David M.	Eugene	OR		

## ASSIGNEE-INFORMATION:

NAME	CITY	STATE	ZIP CODE	COUNTRY	TYPE CODE
InterTrust Technologies Corp.	Santa Clara	CA			02

APPL-NO: 9/ 335465

DATE FILED: June 17, 1999

## PARENT-CASE:

This application is a continuation application of prior application Ser. No. 08/780,393 filed Jan. 8, 1997 now U.S. Pat. No. 5,915,019, which is a continuation application of parent application Ser. No. 08/388,107 filed Feb. 13, 1995, now abandoned, both of which are hereby expressly incorporated by reference.

INT-CL: [7] H04L 9/32

US-CL-ISSUED: 213/153; 380/203, 705/51, 705/58

US-CL-CURRENT: 213/153; 380/203, 705/51, 705/58

FIELD-OF-SEARCH: 705/54, 705/26, 705/400, 705/53, 705/51, 705/52, 705/58, 705/57, 709/300, 380/233, 380/203

## PRIOR-ART-DISCLOSED:

## U.S. PATENT DOCUMENTS

☐ Search Selected☐ Search ALL

PAT-NO	ISSUE-DATE	PATENTEE-NAME	US-CL
<input type="checkbox"/> 3573747	April 1971	Adams et al.	N/A
<input type="checkbox"/> 3609697	September 1971	Blevins	N/A
<input type="checkbox"/> 3796830	March 1974	Smith	N/A
<input type="checkbox"/> 3798359	March 1974	Feistel	N/A
<input type="checkbox"/> 3798360	March 1974	Feistel	N/A

<input type="checkbox"/>	3798605	March 1974	Feistel	N/A
<input type="checkbox"/>	3806882	April 1974	Clarke	N/A
<input type="checkbox"/>	3829833	August 1974	Freeny	N/A
<input type="checkbox"/>	3906448	September 1975	Henriques	N/A
<input type="checkbox"/>	3911397	October 1975	Freeny	N/A
<input type="checkbox"/>	3924065	December 1975	Freeny	N/A
<input type="checkbox"/>	3931504	January 1976	Jacoby	N/A
<input type="checkbox"/>	3946220	March 1976	Brobeck et al.	N/A
<input type="checkbox"/>	3956615	May 1976	Anderson et al.	N/A
<input type="checkbox"/>	3958081	May 1976	Ehrsam et al.	N/A
<input type="checkbox"/>	3970992	July 1976	Boothroyd et al.	N/A
<input type="checkbox"/>	4048619	September 1977	Forman et al.	N/A
<input type="checkbox"/>	4071911	January 1978	Mazur	N/A
<input type="checkbox"/>	4112421	September 1978	Freeny	N/A
<input type="checkbox"/>	4120030	October 1978	Johnstone	N/A
<input type="checkbox"/>	4163280	July 1979	Mori et al.	N/A
<input type="checkbox"/>	4168396	September 1979	Best	N/A
<input type="checkbox"/>	4196310	April 1980	Forman et al.	N/A
<input type="checkbox"/>	4200913	April 1980	Kuhar et al.	N/A
<input type="checkbox"/>	4209787	June 1980	Freeny	N/A
<input type="checkbox"/>	4217588	August 1980	Freeny	N/A
<input type="checkbox"/>	4220991	September 1980	Hamano et al.	N/A
<input type="checkbox"/>	4232193	November 1980	Gerard	N/A
<input type="checkbox"/>	4232317	November 1980	Freeny	N/A
<input type="checkbox"/>	4236217	November 1980	Kennedy	N/A
<input type="checkbox"/>	4253157	February 1981	Kirschner et al.	N/A
<input type="checkbox"/>	4262329	April 1981	Bright et al.	N/A
<input type="checkbox"/>	4265371	May 1981	Desai et al.	N/A
<input type="checkbox"/>	4270182	May 1981	Asija	N/A
<input type="checkbox"/>	4278837	July 1981	Best	N/A
<input type="checkbox"/>	4305131	December 1981	Best	N/A
<input type="checkbox"/>	4306289	December 1981	Lumley	N/A
<input type="checkbox"/>	4309569	January 1982	Merkle	N/A
<input type="checkbox"/>	4319079	March 1982	Best	N/A
<input type="checkbox"/>	4323921	April 1982	Guillou	N/A
<input type="checkbox"/>	4328544	May 1982	Baldwin et al.	N/A
<input type="checkbox"/>	4337483	June 1982	Guillou	N/A
<input type="checkbox"/>	4361877	November 1982	Dyer et al.	N/A

<input type="checkbox"/>	4375579	March 1983	Davidson et al.	N/A
<input type="checkbox"/>	4433207	February 1984	Best	N/A
<input type="checkbox"/>	4434464	February 1984	Suzuki et al.	N/A
<input type="checkbox"/>	4442486	April 1984	Mayer	N/A
<input type="checkbox"/>	4446519	May 1984	Thomas	N/A
<input type="checkbox"/>	4454594	June 1984	Heffron et al.	N/A
<input type="checkbox"/>	4458315	July 1984	Uchenick	N/A
<input type="checkbox"/>	4462076	July 1984	Smith	N/A
<input type="checkbox"/>	4462078	July 1984	Ross	N/A
<input type="checkbox"/>	4465901	August 1984	Best	N/A
<input type="checkbox"/>	4471163	September 1984	Donald et al.	N/A
<input type="checkbox"/>	4484217	November 1984	Block et al.	N/A
<input type="checkbox"/>	4494156	January 1985	Kadison et al.	N/A
<input type="checkbox"/>	4513174	April 1985	Herman	N/A
<input type="checkbox"/>	4528588	July 1985	Lofberg	N/A
<input type="checkbox"/>	4528643	July 1985	Freeny	N/A
<input type="checkbox"/>	4553252	November 1985	Egendorf	N/A
<input type="checkbox"/>	4558176	December 1985	Arnold et al.	N/A
<input type="checkbox"/>	4558413	December 1985	Schmidt et al.	N/A
<input type="checkbox"/>	4562306	December 1985	Chou et al.	N/A
<input type="checkbox"/>	4562495	December 1985	Bond et al.	N/A
<input type="checkbox"/>	4577289	March 1986	Comerford et al.	N/A
<input type="checkbox"/>	4584641	April 1986	Guglielmino	N/A
<input type="checkbox"/>	4588991	May 1986	Atalla	N/A
<input type="checkbox"/>	4589064	May 1986	Chiba et al.	N/A
<input type="checkbox"/>	4593353	June 1986	Pickholtz	N/A
<input type="checkbox"/>	4593376	June 1986	Volk	N/A
<input type="checkbox"/>	4595950	June 1986	Lofberg	N/A
<input type="checkbox"/>	4597058	June 1986	Izumi et al.	N/A
<input type="checkbox"/>	4634807	January 1987	Chorley et al.	N/A
<input type="checkbox"/>	4644493	February 1987	Chandra et al.	N/A
<input type="checkbox"/>	4646234	February 1987	Tolman et al.	N/A
<input type="checkbox"/>	4652990	March 1987	Pailen et al.	N/A
<input type="checkbox"/>	4658093	April 1987	Hellman	N/A
<input type="checkbox"/>	4670857	June 1987	Rackman	N/A
<input type="checkbox"/>	4672572	June 1987	Alsberg	N/A
<input type="checkbox"/>	4677434	June 1987	Fascenda	N/A
<input type="checkbox"/>	4680731	July 1987	Izumi et al.	N/A

<input type="checkbox"/>	4683553	July 1987	Mollier	N/A
<input type="checkbox"/>	4685056	August 1987	Barnsdale et al.	N/A
<input type="checkbox"/>	4688169	August 1987	Joshi	N/A
<input type="checkbox"/>	4691350	September 1987	Kleijne et al.	N/A
<input type="checkbox"/>	4696034	September 1987	Wiedemer	N/A
<input type="checkbox"/>	4701846	October 1987	Ikeda et al.	N/A
<input type="checkbox"/>	4712238	December 1987	Gilhousen et al.	N/A
<input type="checkbox"/>	4713753	December 1987	Boebert et al.	N/A
<input type="checkbox"/>	4740890	April 1988	William	N/A
<input type="checkbox"/>	4747139	May 1988	Taaffe	N/A
<input type="checkbox"/>	4757533	July 1988	Allen et al.	N/A
<input type="checkbox"/>	4757534	July 1988	Matyas et al.	N/A
<input type="checkbox"/>	4768087	August 1988	Taub et al.	N/A
<input type="checkbox"/>	4791565	December 1988	Dunham et al.	N/A
<input type="checkbox"/>	4796181	January 1989	Wiedemer	N/A
<input type="checkbox"/>	4799156	January 1989	Shavit	N/A
<input type="checkbox"/>	4807288	February 1989	Ugon et al.	N/A
<input type="checkbox"/>	4817140	March 1989	Chandra et al.	N/A
<input type="checkbox"/>	4823264	April 1989	Deming	N/A
<input type="checkbox"/>	4827508	May 1989	Shear	N/A
<input type="checkbox"/>	4858121	August 1989	Barber et al.	N/A
<input type="checkbox"/>	4864494	September 1989	Kobus	N/A
<input type="checkbox"/>	4868877	September 1989	Fischer	N/A
<input type="checkbox"/>	4903296	February 1990	Chandra et al.	N/A
<input type="checkbox"/>	4924378	May 1990	Hershey et al.	N/A
<input type="checkbox"/>	4930073	May 1990	Cina	N/A
<input type="checkbox"/>	4949187	August 1990	Cohen	N/A
<input type="checkbox"/>	4977594	December 1990	Shear	N/A
<input type="checkbox"/>	4999806	March 1991	Chernow et al.	N/A
<input type="checkbox"/>	5001752	March 1991	Fischer	N/A
<input type="checkbox"/>	5005122	April 1991	Griffin et al.	N/A
<input type="checkbox"/>	5005200	April 1991	Fischer	N/A
<input type="checkbox"/>	5010571	April 1991	Katznelson	N/A
<input type="checkbox"/>	5023907	June 1991	Johnson et al.	N/A
<input type="checkbox"/>	5047928	September 1991	Wiedemer	N/A
<input type="checkbox"/>	5048085	September 1991	Abraham et al.	N/A
<input type="checkbox"/>	5050213	September 1991	Shear	N/A
<input type="checkbox"/>	5091966	February 1992	Bloomberg et al.	N/A

<input type="checkbox"/>	5103392	April 1992	Mori	N/A
<input type="checkbox"/>	5103476	April 1992	Waite et al.	N/A
<input type="checkbox"/>	5111390	May 1992	Ketcham	N/A
<input type="checkbox"/>	5119493	June 1992	Janis et al.	N/A
<input type="checkbox"/>	5128525	July 1992	Stearns et al.	N/A
<input type="checkbox"/>	5136643	August 1992	Fischer	N/A
<input type="checkbox"/>	5136646	August 1992	Haber et al.	N/A
<input type="checkbox"/>	5136647	August 1992	Haber et al.	N/A
<input type="checkbox"/>	5136716	August 1992	Harvey et al.	N/A
<input type="checkbox"/>	5146575	September 1992	Nolan	N/A
<input type="checkbox"/>	5148481	September 1992	Abraham et al.	N/A
<input type="checkbox"/>	5155680	October 1992	Wiedemer	N/A
<input type="checkbox"/>	5163091	November 1992	Graziano et al.	N/A
<input type="checkbox"/>	5168147	December 1992	Bloomberg	N/A
<input type="checkbox"/>	5185717	February 1993	Mori	N/A
<input type="checkbox"/>	5201046	April 1993	Goldberg et al.	N/A
<input type="checkbox"/>	5201047	April 1993	Maki et al.	N/A
<input type="checkbox"/>	5208748	May 1993	Flores et al.	N/A
<input type="checkbox"/>	5214702	May 1993	Fischer	N/A
<input type="checkbox"/>	5216603	June 1993	Flores et al.	N/A
<input type="checkbox"/>	5221833	June 1993	Hecht	N/A
<input type="checkbox"/>	5222134	June 1993	Waite et al.	N/A
<input type="checkbox"/>	5224160	June 1993	Paulini et al.	N/A
<input type="checkbox"/>	5224163	June 1993	Gasser et al.	N/A
<input type="checkbox"/>	5235642	August 1993	Wobber et al.	N/A
<input type="checkbox"/>	5245165	September 1993	Zhang	N/A
<input type="checkbox"/>	5247575	September 1993	Sprague et al.	N/A
<input type="checkbox"/>	5260999	November 1993	Wyman	N/A
<input type="checkbox"/>	5263158	November 1993	Janis	N/A
<input type="checkbox"/>	5265164	November 1993	Matyas et al.	N/A
<input type="checkbox"/>	5276735	January 1994	Boebert et al.	N/A
<input type="checkbox"/>	5280479	January 1994	Mary	N/A
<input type="checkbox"/>	5285494	February 1994	Sprecher et al.	N/A
<input type="checkbox"/>	5301231	April 1994	Abraham et al.	N/A
<input type="checkbox"/>	5311591	May 1994	Fischer	N/A
<input type="checkbox"/>	5319705	June 1994	Halter et al.	N/A
<input type="checkbox"/>	5319785	June 1994	Halter et al.	N/A
<input type="checkbox"/>	5337360	August 1994	Fischer	N/A

<input type="checkbox"/>	5341429	August 1994	Stringer et al.	N/A
<input type="checkbox"/>	5343527	August 1994	Moore et al.	N/A
<input type="checkbox"/>	5347579	September 1994	Blandford	N/A
<input type="checkbox"/>	5351293	September 1994	Michener et al.	N/A
<input type="checkbox"/>	5355474	October 1994	Thuraisingham et al.	N/A
<input type="checkbox"/>	5373561	December 1994	Haber et al.	N/A
<input type="checkbox"/>	5390247	February 1995	Fischer	N/A
<input type="checkbox"/>	5390330	February 1995	Talati	N/A
<input type="checkbox"/>	5392220	February 1995	van den Hamer et al.	N/A
<input type="checkbox"/>	5392390	February 1995	Crozier	N/A
<input type="checkbox"/>	5394469	February 1995	Nagel et al.	N/A
<input type="checkbox"/>	5410598	April 1995	Shear	N/A
<input type="checkbox"/>	5412717	May 1995	Fischer	N/A
<input type="checkbox"/>	5421006	May 1995	Jablon	N/A
<input type="checkbox"/>	5422953	June 1995	Fischer	N/A
<input type="checkbox"/>	5428606	June 1995	Moskowitz	N/A
<input type="checkbox"/>	5438508	August 1995	Wyman	N/A
<input type="checkbox"/>	5442645	August 1995	Ugon	N/A
<input type="checkbox"/>	5444779	August 1995	Daniele	N/A
<input type="checkbox"/>	5449895	September 1995	Hecht et al.	N/A
<input type="checkbox"/>	5449896	September 1995	Hecht et al.	N/A
<input type="checkbox"/>	5450493	September 1995	Maher	N/A
<input type="checkbox"/>	5453601	September 1995	Rosen	N/A
<input type="checkbox"/>	5453605	September 1995	Hecht et al.	N/A
<input type="checkbox"/>	5455407	October 1995	Rosen	N/A
<input type="checkbox"/>	5455861	October 1995	Faucher et al.	N/A
<input type="checkbox"/>	5455953	October 1995	Russell	N/A
<input type="checkbox"/>	5457746	October 1995	Dolphin	N/A
<input type="checkbox"/>	5463565	October 1995	Cookson et al.	N/A
<input type="checkbox"/>	5473687	December 1995	Lipscomb et al.	N/A
<input type="checkbox"/>	5473692	December 1995	Davis	N/A
<input type="checkbox"/>	5479509	December 1995	Ugon	N/A
<input type="checkbox"/>	5485622	January 1996	Yamaki	N/A
<input type="checkbox"/>	5491800	February 1996	Goldsmith et al.	N/A
<input type="checkbox"/>	5497479	March 1996	Hornbuckle	N/A
<input type="checkbox"/>	5497491	March 1996	Mitchell et al.	N/A
<input type="checkbox"/>	5499298	March 1996	Narasimhalu et al.	N/A
<input type="checkbox"/>	5504757	April 1996	Cook et al.	N/A

<input type="checkbox"/>	5504818	April 1996	Okano	N/A
<input type="checkbox"/>	5504837	April 1996	Griffeth et al.	N/A
<input type="checkbox"/>	5508913	April 1996	Yamamoto et al.	N/A
<input type="checkbox"/>	5509070	April 1996	Schull	N/A
<input type="checkbox"/>	5513261	April 1996	Maher	N/A
<input type="checkbox"/>	5530235	June 1996	Stefik et al.	N/A
<input type="checkbox"/>	5530752	June 1996	Rubin	N/A
<input type="checkbox"/>	5533123	July 1996	Force et al.	N/A
<input type="checkbox"/>	5534975	July 1996	Stefik et al.	N/A
<input type="checkbox"/>	5537526	July 1996	Anderson et al.	N/A
<input type="checkbox"/>	5539735	July 1996	Moskowitz	N/A
<input type="checkbox"/>	5539828	July 1996	Davis	N/A
<input type="checkbox"/>	5550971	August 1996	Brunner et al.	N/A
<input type="checkbox"/>	5553282	September 1996	Parrish et al.	N/A
<input type="checkbox"/>	5557518	September 1996	Rosen	N/A
<input type="checkbox"/>	5563946	October 1996	Cooper et al.	N/A
<input type="checkbox"/>	5568552	October 1996	Davis	N/A
<input type="checkbox"/>	5572673	November 1996	Shurts	N/A
<input type="checkbox"/>	5592549	January 1997	Nagel et al.	N/A
<input type="checkbox"/>	5606609	February 1997	Houser et al.	N/A
<input type="checkbox"/>	5613004	March 1997	Cooperman et al.	N/A
<input type="checkbox"/>	5621797	April 1997	Rosen	N/A
<input type="checkbox"/>	5629980	May 1997	Stefik et al.	N/A
<input type="checkbox"/>	5633932	May 1997	Davis et al.	N/A
<input type="checkbox"/>	5634012	May 1997	Stefik et al.	N/A
<input type="checkbox"/>	5636292	June 1997	Rhoads	N/A
<input type="checkbox"/>	5638443	June 1997	Stefik	N/A
<input type="checkbox"/>	5638504	June 1997	Scott et al.	N/A
<input type="checkbox"/>	5640546	June 1997	Gopinath et al.	N/A
<input type="checkbox"/>	5655077	August 1997	Jones et al.	N/A
<input type="checkbox"/>	5687236	November 1997	Moskowitz et al.	N/A
<input type="checkbox"/>	5689587	November 1997	Bender et al.	N/A
<input type="checkbox"/>	5692180	November 1997	Lee	N/A
<input type="checkbox"/>	5710834	January 1998	Rhoads	N/A
<input type="checkbox"/>	5740549	April 1998	Reilly et al.	N/A
<input type="checkbox"/>	5745604	April 1998	Rhoads	N/A
<input type="checkbox"/>	5748763	May 1998	Rhoads	N/A
<input type="checkbox"/>	5748783	May 1998	Rhoads	N/A

<input type="checkbox"/> 5748960	May 1998	Fischer	N/A
<input type="checkbox"/> 5754849	May 1998	Dyer et al.	N/A
<input type="checkbox"/> 5757914	May 1998	McManis	N/A
<input type="checkbox"/> 5758152	May 1998	LeTourneau	N/A
<input type="checkbox"/> 5765152	June 1998	Erickson	N/A
<input type="checkbox"/> 5768426	June 1998	Rhoads	N/A
<input type="checkbox"/> 5915019	June 1999	Ginter et al.	705/54

## FOREIGN PATENT DOCUMENTS

FOREIGN-PAT-NO	PUBN-DATE	COUNTRY	US-CL
62-241061	December 1984	BEX	
9 004 79	December 1984	BEX	
3803982A1	January 1990	DEX	
0 084 441 A1	July 1983	EPX	
0 128 672 A1	December 1984	EPX	
0 135 422 A1	March 1985	EPX	
0 180 460 A1	May 1986	EPX	
0 370 146 A1	November 1988	EPX	
0 399 822 A2	November 1990	EPX	
0 421 409 A2	April 1991	EPX	
0 456 386 A2	November 1991	EPX	
0 469 864 A2	February 1992	EPX	
0 565 314 A2	October 1993	EPX	
0 593 305 A2	April 1994	EPX	
0 651 554 A1	May 1995	EPX	
0 668 695 A2	August 1995	EPX	
0 695 985 A1	February 1996	EPX	
0 696 798 A1	February 1996	EPX	
0 714 204 A2	May 1996	EPX	
0 715 243 A1	June 1996	EPX	
0 715 244 A1	June 1996	EPX	
0 715 245 A1	June 1996	EPX	
0 715 246 A1	June 1996	EPX	
0 715 247 A1	June 1996	EPX	
0 725 376 A2	August 1996	EPX	
0 763 936 A2	September 1996	EPX	
0 749 081 A1	December 1996	EPX	
0 778 513 A2	June 1997	EPX	
0 795 873 A2	September 1997	EPX	
0 800 312 A1	October 1997	EPX	
2136175	September 1984	GBX	
2264796A	September 1993	GBX	
2294348	April 1996	GBX	
2295947	June 1996	GBX	
57-726	May 1982	JPX	
62-225059	August 1987	JPX	
62-241061	October 1987	JPX	
1-068835	March 1989	JPX	
64-68835	March 1989	JPX	

2-242352	September 1990	JPX
2-247763	October 1990	JPX
2-294855	December 1990	JPX
4-369068	December 1992	JPX
5-181734	July 1993	JPX
5-257783	October 1993	JPX
5-268415	October 1993	JPX
6-175794	June 1994	JPX
6-215010	August 1994	JPX
7-056794	March 1995	JPX
7-084852	March 1995	JPX
7-141138	June 1995	JPX
7-200317	August 1995	JPX
7-200492	August 1995	JPX
7-244639	September 1995	JPX
8-137795	May 1996	JPX
8-152990	June 1996	JPX
8-185292	July 1996	JPX
8-185298	July 1996	JPX
WO 95/02310	May 1985	WOX
WO 85/03584	August 1985	WOX
WO 90/02382	March 1990	WOX
WO 92/06438	April 1992	WOX
WO 92/22870	December 1992	WOX
WO 93/01550	January 1993	WOX
WO 94/01821	January 1994	WOX
WO 94/03859	February 1994	WOX
WO 94/06103	March 1994	WOX
WO 94/16395	July 1994	WOX
WO 94/18620	August 1994	WOX
WO 94/22266	September 1994	WOX
WO 94/27406	November 1994	WOX
WO 96/13013	May 1995	WOX
WO 95/14289	May 1995	WOX
WO 96/00963	January 1996	WOX
WO 96/06503	February 1996	WOX
WO 96/03835	February 1996	WOX
WO 96/05698	February 1996	WOX
WO 96/21192	July 1996	WOX
WO 96/24092	August 1996	WOX
WO 97/03423	January 1997	WOX
WO 97/07656	March 1997	WOX
WO 97/25816	July 1997	WOX
WO 97/32251	September 1997	WOX
WO 97/48203	December 1997	WOX

## OTHER PUBLICATIONS

David Arneke and Donna Cunningham, Document from the Internet: AT&T encryption system protects information services, (News Release), Jan. 9, 1995, 1 page.  
Claude Baggett, Cable's Emerging Role in the Information Superhighway, Cable Labs, (undated), 13 slides.  
Theodore Sedgwick Barassi, Document from Internet: The Cybernotary: Public Key Registration and Certification and Authentication of International Legal Transactions, (undated), 4 pages.

Hugh Barnes, memo to Henry LaMuth, subject: George Gilder articles, May 31, 1994, 2 pages.

Comments in the Matter of Public Hearing and Request for Comments on the International Aspects of the National Information Infrastructure, Before the Department of Commerce, Aug. 12, 1994, pp. 1-15 (comments of Dan Bart).

Michael Baum, "Worldwide Electronic Commerce: Law, Policy and Controls Conference," Nov. 11, 1993, 18 pages.

Robert M. Best, Preventing Software Piracy With Crypto-Microprocessors, Digest of Papers, VLSI: New Architectural Horizons, Feb. 1980, pp. 466-469.

Richard L. Bisbey, II and Gerald J. Popek, Encapsulation: An Approach to Operating System Security, (USC/Information Science Institute, Marina Del Rey, CA), Oct. 1973, pp. 666-675.

Rolf Blom, Robert Forchheimer, et al., Encryption Methods in Data Networks, Ericsson Technics, No. 2, Stockholm, Sweden, 1978.

Rick E. Bruner, Document from the Internet: PowerAgent, NetBot help advertisers reach Internet shoppers, Aug. 1997, 3 pages.

Denise Caruso, Technology, Digital Commerce: 2 plans for watermarks, which can bind proof of authorship to electronic works, N.Y. Times, Aug. 7, 1995, p. D5.

A.K. Choudhury, N. F. Maxemchuck, et al., Copyright Protection for Electronic Publishing Over Computer Networks, (AT&T Bell Laboratories, Murray Hill, N. J.) Jun. 1994, 17 pages.

Tim Clark, Ad service gives cash back, Document from the Internet: (visited Aug. 4, 1997), 2 pages.

Donna Cunningham, David Arneke, et al., Document from the Internet: AT&T, VLSI Technology join to improve info highway security, (News Release) Jan. 31, 1995, 3 pages.

Lorcan Dempsey and Stuart Weibel, The Warwick Metadata Workshop: A Framework for the Deployment of Resource Description, D-Lib Magazine, Jul. 15, 1996.

Dorothy E. Denning and Peter J. Denning, Data Security, 11 Computing Surveys No. 3, Sep. 1979, pp. 227-249.

Whitfield Diffie and Martin E. Hellman, New Directions in Cryptography, IEEE Transactions on Information Theory, vol. 22, No. 6, Nov. 1976, pp. 644-651.

Whitfield Diffie and Martin E. Hellman, Privacy and Authentication: An Introduction to Cryptography, Proceedings of the IEEE, vol. 67, No. 3, Mar. 1979, pp. 397-427.

Stephen R. Dusse and Burton S. Kaliski, A Cryptographic Library for the Motorola 56000, Advances in Cryptology--Proceedings of Eurocrypt 90, (I.M. Damgard, ed., Springer-Verlag) 1991, pp. 230-244.

Esther Dyson, Intellectual Value, WIRED Magazine, Jul. 1995, pp. 136-141 and 182-183.

Science, space and technology, Hearing before Subcomm. on Technology, Environment, and Aviation, May 26, 1994 (testimony of D. Linda Garcia).

James Gleick, Dead as a Dollar, The New York Times Magazine, Jun. 16, 1996, Sect. 6, pp. 26-30, 35, 42, 50, 54.

Fred Greguras, Document from Internet: Softic Symposium '95, Copyright Clearances and Moral Rights, Dec. 11, 1995, 3 pages.

Louis C. Guillou, Smart Cards and Conditional Access, Advances in Cryptography--Proceedings of EuroCrypt 84 (T. Beth et al, Ed., Springer-Verlag, 1985) pp. 480-490.

Harry H. Harman, Modern Factor Analysis, Third Edition Revised, University of Chicago Press, Chicago and London, 1976.

Amir Herzberg and Shlomit S. Pinter, Public Protection of Software, ACM Transactions on Computer Systems, vol. 5, No. 4, Nov. 1987, pp. 371-393.

Jud Hofmann, Interfacing the NII to User Homes, (Consumer Electronic Bus. Committee) NIST, Jul. 1994, 12 slides.

Jud Hofmann, Interfacing the NII to User Homes, Electronic Industries Association, (Consumer Electronic Bus Committee) (undated), 14 slides.

Stannie Holt, Document from the Internet: Start-up promises user confidentiality in Web marketing service, InfoWorld Electric News (updated Aug. 13, 1997).

Jay J. Jiang and David W. Conrath, A Concept-based Approach to Retrieval from an Electronic Industrial Directory, International Journal of Electronic Commerce, vol. 1, No. 1 (Fall 1996) pp. 51-72.

Debra Jones, Document from the Internet: Top Tech Stories, PowerAgent Introduces First Internet `Informediary` to Empower and Protect Consumers, (updated Aug. 13, 1997) 3 pages.

Kevin Kelly, E-Money, Whole Earth Review, Summer 1993, pp. 40-59.

Stephen Thomas Kent, Protecting Externally Supplied Software in Small Computers, (MIT/LCS/TR-255) Sep. 1980 254 pages.

David M. Kristol, Steven H. Low and Nicholas F. Maxemchuk, Anonymous Internet Mercantile Protocol, (AT&T Bell Laboratories, Murray Hill, NJ) Draft: Mar. 17, 1994.

Carl Lagoze, The Warwick Framework, A Container Architecture for Diverse Sets of Metadata, D-Lib Magazine, Jul./Aug. 1996.

Mike Lanza, e-mail, George Gilder's Fifth Article--Digital Darkhorse--Newspapers, Feb. 21, 1994.

Steven Levy, E-Money, That's What I want, WIRED, Dec. 1994, 10 pages.

Steven H. Low and Nicholas F. Maxemchuk, Anonymous Credit Cards, AT&T Bell Laboratories, Proceedings of the 2.sup.nd ACM Conference on Computer and Communication Security, Fairfax, VA, Nov. 2-4, 1994, 10 pages.

Steven H. Low, Nicholas F. Maxemchuk, and Sanjoy Paul, Anonymous Credit Cards and its Collusion Analysis (AT&T Bell Laboratories, Murray Hill, N.J.) Oct. 10, 1994, 18 pages.

S. H. Low, N.F. Maxemchuk, et al., Document Marking and Identification using both line and word Shifting (AT&T Bell Laboratories, Murray Hill, N.J.) Jul. 29, 1994, 22 pages.

Malcolm MacLachlan, Document from the Internet: PowerAgent Debuts Spam-Free Marketing, TechWire, Aug. 13, 1997, 3 pages.

N.F. Maxemchuk, Electronic Document Distribution, (AT&T Bell Laboratories, Murray Hill, N.J.) (undated).

Eric Milbrandt, Document from the Internet: Steganography Info and Archive, 1996, 2 pages.

Ryoichi Mori and Masaji Kawahara, Superdistribution: The Concept and the Architecture, The Transactions of The EIEICE, V, E73, No. 7, Tokyo, Japan, Jul. 1990.

Walter S. Mossberg, Personal Technology, Threats to Privacy On-Line Become More Worrisome, The Wall Street Journal, Oct. 24, 1996.

Nicholas Negroponte, Some Thoughts on Likely and Expected Communications Scenarios: A Rebuttal, Telecommunications, Jan. 1993, pp. 41-42.

Nicholas Negroponte, Electronic Word of Mouth, WIRED, Oct. 1996, p. 218.

Peter G. Neumann, Robert S. Boyer, et al., A Provably Secure Operating System: The System, Its Applications, and Proofs, Computer Science Laboratory Report CSL-116, Second Edition, SRI International, Jun. 1980.

Joseph N. Pelton (Dr.), Why Nicholas Negroponte is Wrong About the Future of Telecommunication, Telecommunications, Jan. 1993, pp. 35-40.

Gordon Rankine (Dr.), Thomas--A Complete Single-Chip RSA Device, Advances in Cryptography, Proceedings of CRYPTO 86, (A.M. Odizko Ed., Springer-Verlag) 1987, pp. 480-487.

Arthur K. Reilly, Input to the `International Telecommunications Hearings,` Panel 1: Component Technologies of the NII/GII, Standards Committee T1-Telecommunications (undated).

Paul Resnick and Hal R. Varion, Recommender Systems, Communications of the ACM, vol. 40, No. 3, Mar. 1997 pp. 56-89.

Lance Rose, Cyberspace and the Legal Matrix: Laws or Confusion?, 1991.

Steve Rosenthal, Interactive Network: Viewers Get Involved, New Media, Dec. 1992, pp. 30-31.

Steve Rosenthal, Interactive TV: The Gold Rush is on, New Media, Dec. 1992, pp. 27-29.

Steve Rosenthal, Mega Channels, New Media, Sep. 1993, pp. 36-46.

Edward Rothstein, Technology, Connections, Making the Internet come to you through `push` technology, N. Y. Times, Jan. 20, 1997, p. D5.

Ken Rutkowski, Document from Internet: PowerAgent Introduces First Internet `Informediary` to Empower and Protect Consumers, Tech Talk News Story, Aug. 4, 1997, 1 page.

Ira Sager (Edited by), Bits & Bytes, Business Week, Sep. 23, 1996, p. 142E.

Schlosstein, Steven, America: The G7's Comeback Kid, International Economy, Jun./Jul. 1993, 5 pages.

Ingrid Scnaumueller-Bichl and Ernst Piller, A Method of Software Protection Based on the Use of Smart Cards and Cryptographic Techniques, (undated), 9 pages.

Jurgen Schurmann, Pattern Classification, A Unified View of Statistical and Neural Approaches, John Wiley & Sons, Inc., 1996.

Victor Shear, Solutions for CD-ROM Pricing and Data Security Problems, CD ROM Yearbook 1988-1989 (Microsoft Press 1988 or 1989), pp. 530-533.

Karl Siuda, Security Services in Telecommunications Networks, Seminar: Mapping New Applications Onto New Technologies, edited by B. Plattner and P Gunzburger; Zurich, Mar. 8-10, 1988, pp. 45-52, XP000215989.

Sean Smith and J.D. Tygar, Signed Vector Timestamps: A Secure Protocol for

Partial Order Time, CMU-93-116, School of Computer Science Carnegie Mellon University, Pittsburgh, Pennsylvania, Oct. 1991; version of Feb. 1993, 15 pages.

Mark Stefik, Letting Loose the Light: Igniting Commerce in Electronic Publication, (Xerox PARC, Palo Alto, CA) 1994-1995, 35 pages.

Mark Stefik, Letting Loose the Light: Igniting Commerce In Electronic Publication, Internet Dreams: Archetypes, Myths, and Metaphors. Massachusetts Institute of Technology, 1996, pp. 219-253.

Mark Stefik, Chapter 7, Classification, Introduction to Knowledge Systems (Morgan Kaufmann Publishers, Inc., 1995) pp. 543-607.

Tom Stephenson, The Info Infrastructure Initiative: Data Super Highways and You, Advanced Imaging, May 1993, pp. 73-74.

Bruce Sterling, Literary freeware: Not for Commercial Use, remarks at Computers, Freedom and Private Conference IV, Chicago, IL, Mar. 26, 1994.

Bruno Struif, The Use of Chipcards for Electronic Signatures and Encryption, Proceedings of the 1989 Conference on VSLI and Computer Peripherals, IEEE Computer Society Press, 1989, pp. (4)155-(4)158.

J.D. Tygar and Bennet Yee, Cryptography: It's Not Just For Electronic Mail Anymore, CMU-CS-93-107, School of Computer Science Carnegie Mellon University, Pittsburgh, PA, Mar. 1, 1993, 21 pages.

J.D. Tygar and Bennet Yee, Dyad: A System for Using Physically Secure Coprocessors, School of Computer Science, Carnegie Mellon University, Pittsburgh, PA (undated), 41 pages.

J.D. Tygar and Bennet Yee, Dyad: A System for Using Physically Secure Coprocessors, School of Computer Science, Carnegie Mellon University, Pittsburgh, PA, May 1991, 36 pages.

T. Valovic, The Role of Computer Networking in the Emerging Virtual Marketplace, Telecommunications, (undated), pp. 40-44.

Joan Voight, Beyond the Banner, Wired, Dec. 1996, pp. 196, 200, 204.

Steven Vonder Haar, Document from the Internet: PowerAgent Launches Commercial Service, Interactive Week, Aug. 4, 1997, 1 page.

Robert Weber, Metering Technologies for Digital Intellectual Property, A Report to the International Federation of Reproduction Rights Organisations (Boston, MA), Oct. 1994, pp. 1-29.

Robert Weber, Document from the Internet: Digital Rights Management Technologies, Oct. 1995, 21 pages.

Robert Weber, Digital Rights Management Technologies, A Report to the International Federation of Reproduction Rights Organisations, Northeast Consulting Resources, Inc., Oct. 1995, 49 pages.

Adele Weder, Life on the Infohighway, INSITE, (undated), pp. 23-25.

Steve H. Weingart, Physical Security for the ABYSS System, (IBM Thomas J.

Watson Research Center, Yorktown Heights, NY), 1987, pp. 52-58.

Daniel J. Weitzner, A Statement on EFF's Open Platform Campaign as of Nov., 1993, 3 pages.

Steve R. White, ABYSS: A Trusted Architecture for Software Protection, (IBM Thomas J. Watson Research Center, Yorktown Heights, NY), 1987, pp. 38-50.

Bennet Yee, Using Secure Coprocessors, CMU-CS-94-149, School of Computer Science, Carnegie Mellon University, Pittsburgh, PA, 1994, 94 pages.

Frank Yellin, Document from the Internet: Low Level Security in Java, Sun Microsystems, 1996, 8 pages.

Symposium: Applications Requirements for Innovative Video Programming; How to Foster (or Cripple) Program Development Opportunities for Interactive Video Programs Delivered on Optical Media: A Challenge for the Introduction of DVD (Digital Video Disc) (Oct. 19-20, 1995, Sheraton Universal Hotel, Universal City CA).

Argent Information, Q&A Sheet, Document from the Internet: , Copyright 1995, The DICE Company, (last modified Jun. 16, 1996), 7 pages.

New Products, Systems and Services, AT&T Technology, vol. 9, No. 4, (undated), pp. 16-19.

Cable Television and America's Telecommunications Infrastructure, (National Cable Television Association, Washington, D.C.), Apr. 1993, 19 pages.

CD ROM: Introducing . . . The Workflow CD-ROM Sampler (Creative Networks, MCIMail: Creative Networks, Inc.), (undated).

Codercard, Basic Coder Subsystem (Interstate Electronics Corp., Anaheim, CA), (undated) 4 pages.

Collection of documents including: Protecting Electronically Published Properties, Increasing Publishing Profits, (Electronic Publishing Resources Inc.,) Jan. 1993, 25 pages.

Communications of the ACM, vol. 39, No. 6, Jun. 1996, 130 pages.

Communications of the ACM, "Intelligent Agents," vol. 37, No. 7, Jul. 1994, 170 pages.

Computer Systems Policy Project (CSSP), Perspectives on the National Information Infrastructure: Ensuring Interoperability, Feb. 1994, 5 slides.

DiscStore (Electronic Publishing Resources, Chevy Chase, MD), 1991.

DSP56000/DSP56001 Digital Signal Processor User's Manual, (Motorola), 1990, p. 2-2.

A Supplement to Midrange Systems, Premenos Corp. White Paper: The Future of Electronic Commerce, Document from Internet: , Aug. 1995, 4 pages.

CGI Common Gateway Interface, Document from the Internet: , 1996, 1 page.

HotJava.TM.: The Security Story, Document from the Internet: (undated) 4 pages.

About the Digital Notary Service, Document from the Internet: , (Surety Technologies), 1994-5, 6 pages.

Templar Overview: Premenos, Document from the Internet: (undated), 4 pages.

Templar Software and Services, Secure, Reliable, Standards-Based EDI Over the Internet: Document from the Internet: (Premenos) (undated), 1 page.

JAVASOFT, Frequently Asked Questions--Applet Security, Document from Internet: , Jun. 7, 1996, 8 pages.

News from The Document Company Xerox, Xerox Announces Software Kit for Creating `Working Documents` with Dataglyphs Document from Internet: Nov. 6, 1995, 13 pages.

Premenos Announces Templar 2.0--Next Generation Software for Secure Internet EDI, Document from Internet: , Jan. 17, 1996, 1 page.

WEPIN Store, Stenography (Hidden, Writing), Document from Internet: (Common Law), 1995, 1 page.

Sag's durch die Blume, Document from Internet: (German), (undated), 5 pages.

A Publication of the Electronic Frontier Foundation, EFFector Online vol. 6 No. 6., Dec. 6, 1993, 8 pages.

EIA and TIA White Paper on National Information Infrastructure, The Electronic Industries Association and the Telecommunications Industry Association, Washington, D.C., (undated).

Electronic Currency Requirements, XIWT (Cross Industry Working Group), (undated).

Electronic Publishing Resources Inc. Protecting Electronically Published Properties Increasing Publishing Profits (Electronic Publishing Resources, Chevy Chase, MD) 1991, 19 pages.

What is Firefly?, Document from the Internet: , (Firefly Network, Inc.) Firefly revision: 41.4, (Copyright 1995, 1996), 1 page.

First CII Honeywell Bull International Symposium on Computer Security and Confidentiality, Conference Text, Jan. 26-28, 1981, pp. 1-21.

Framework for National Information Infrastructure Services, Draft, U.S. Department of Commerce, Jul. 1994.

Framework for National Information Infrastructure Services, NIST, Jul. 1994, 12 Slides.

Intellectual Property and the National Information Infrastructure, a Preliminary Draft of the Report of the Working Group on Intellectual Property Rights, Green paper, Jul. 1994, 141 pages.

Multimedia Mixed Object Envelopes Supporting a Graduated Fee Scheme Via Encryption, IBM Technical Disclosure Bulletin, vol. 37, No. 3, Mar. 1, 1994, pp. 413-417, XP000441522.

Transformer Rules Strategy for Software Distribution Mechanism-Support Products, IBM Technical Disclosure Bulletin, vol. 37, No. 48, Apr. 1994, pp. 523-525, XP000451335.

IISP Break Out Session Report for Group No. 3, Standards Development and Tracking System, (undated).

Information Infrastructure Standards Panel: NII "The Information Superhighway", NationsBank--HGDeal--ASC X9, (undated), 15 pages.

Invoice? What's an Invoice?, Business Week, Jun. 10, 1996, pp. 110-112.

Micro Card (Micro Card Technologies, Inc., Dallas, TX), (undated), 4 pages.

Background on the Administration's Telecommunications Policy Reform Initiative, News Release, The White House, Office of the President, Jan. 11, 1994, 7 pages.

NII, Architecture Requirements, XIWT, (undated).

Symposium: Open System Environment Architectural Framework for National Information Infrastructure Services and Standards, in Support of National Class Distributed Systems, Distributed System Engineering Program Sponsor Group, Draft 1.0, Aug. 5, 1994, 34 pages.

Proper Use of Consumer Information on the Internet, Document from the Internet,

White Paper, (PowerAgent Inc., Menlo Park, CA) Jun. 1997, 9 pages.  
What the Experts are Reporting on PowerAgent, Document from the Internet,  
PowerAgent Press Releases, Aug. 13, 1997, 6 pages.  
What the Experts are Reporting on PowerAgent, Document from the Internet,  
PowerAgent Press Releases, Aug. 4, 1997, 5 pages.  
Portland Software's Ziplock, Internet Information, Copyright Portland Software  
1996-1997, 12 pages.  
Press Release, National Semiconductor and EPR Partner for Information  
Metering/Data Security Cards (Mar. 4, 1994).  
R01 (Personal Library Software, 1987 or 1988).  
R01--Solving Critical Electronics Publishing Problems (Personal Library  
Software, 1987 or 1988).  
Serving the Community: A Public Interest Vision of the National Information  
Infrastructure, Computer Professionals for Social Responsibility, Executive  
Summary (undated).  
Special Report, The Internet: Fulfilling the Promise; Lynch, Clifford, The  
Internet Bringing Order From Chaos; Resnick, Paul, Search the Internet, Hearst,  
Marti A., Filtering Information on the Internet; Stefik, Mark, Interfaces for  
Searching the Web; Scientific American, Mar. 1997, pp. 49-56, 62-67, 68-72,  
78-81.  
The 1.1 Future of the Electronic Marketplace: Return to a Hunting and Gathering  
Society, (undated), 2 pages.  
The Benefits of RDI for Database Protection and usage Based Billing (Personal  
Library Software, 1987 or 1988).  
The New Alexandria No. 1, Alexandria Institute, Jul.-Aug. 1986, pp. 1-12.  
Is Advertising Really Dead?, Wired 1.02, Part 2, 1994.  
How Can I Put an Access Counter on My Home Page?, World Wide Web FAQ, 1996, 1  
page.  
XIWT Cross Industry Working Team, Jul. 1994, 5 pages.

ART-UNIT: 211

PRIMARY-EXAMINER: Barron, Jr.; Gilberto

ATTY-AGENT-FIRM: Finnegan, Henderson, Farabow, Garrett & Dunner, L.L.P.

#### ABSTRACT:

The present invention provides systems and methods for secure transaction management and electronic rights protection. Electronic appliances such as computers equipped in accordance with the present invention help to ensure that information is accessed and used only in authorized ways, and maintain the integrity, availability, and/or confidentiality of the information. Such electronic appliances provide a distributed virtual distribution environment (VDE) that may enforce a secure chain of handling and control, for example, to control and/or meter or otherwise monitor use of electronically stored or disseminated information. Such a virtual distribution environment may be used to protect rights of various participants in electronic commerce and other electronic or electronic-facilitated transactions. Distributed and other operating systems, environments and architectures, such as, for example, those using tamper-resistant hardware-based processors, may establish security at each node. These techniques may be used to support an all-electronic information distribution, for example, utilizing the "electronic highway."

8 Claims, 155 Drawing figures

**WEST**☐ **Generate Collection**

L7: Entry 1 of 4

File: DWPI

Jul 19, 2001

DERWENT-ACC-NO: 2001-496746

DERWENT-WEEK: 200168

COPYRIGHT 2001 DERWENT INFORMATION LTD

TITLE: Digital rights management system operating on computing device when user requests an encrypted digital content to be rendered by the computer

INVENTOR: GANESAN, K; LIU, D ; PEINADO, M

PATENT-ASSIGNEE:

ASSIGNEE

CODE

MICROSOFT CORP

MICT

PRIORITY-DATA: 2000US-0526290 (March 15, 2000), 2000US-176425P (January 14, 2000)

PATENT-FAMILY:

PUB-NO	PUB-DATE	LANGUAGE	PAGES	MAIN-IPC
WO 200152021 A1	July 19, 2001	E	126	G06F001/00
AU 200069281 A	July 24, 2001		000	G06F001/00

DESIGNATED-STATES: AE AG AL AM AT AU AZ BA BB BG BR BY CA CH CN CR CU CZ DE DK DM DZ EE ES FI GB GD GE GH GM HR HU ID IL IN IS JP KE KG KP KR KZ LC LK LR LS LT LU LV MD MG MK MN MW MX MZ NO NZ PL PT RO RU SD SE SG SI SK SL TJ TM TR TT TZ UA UG UZ VN YU ZA ZW AT BE CH CY DE DK EA ES FI FR GB GH GM GR IE IT KE LS LU MC MW MZ NL OA PT SD SE SL SZ TZ UG ZW

APPLICATION-DATA:

PUB-NO	APPL-DATE	APPL-NO	DESCRIPTOR
WO 200152021A1	August 22, 2000	2000WO-US23108	
AU 200069281A	August 22, 2000	2000AU-0069281	
AU 200069281A		WO 200152021	Based on

INT-CL (IPC): G06F 1/00

RELATED-ACC-NO: 2001-522158;2001-522159 ;2001-596328 ;2001-596397

ABSTRACTED-PUB-NO: WO 200152021A

BASIC-ABSTRACT:

NOVELTY - Uses a black box (30) in the digital rights management (DRM) system for performing decryption and encryption functions. The black box contains identifier of computing device (14) and is tied to the computing device.

DETAILED DESCRIPTION - The black box also contains at least one black box public key. The DRM system also contains digital license (16) corresponding to the digital content. The licence includes a decryption key (KD) for decrypting the encrypted digital content. The decryption key is encrypted according to a black box public key of the black box. The licence is tied to the black box, and the computing device. AN INDEPENDENT CLAIM is made for a method of

operating DRM system when user requests that computer renders an encrypted digital content.

USE - For enforcing rights in a digital content allowing access to encrypted digital content only in accordance with parameters specified by licence rights acquired by user.

ADVANTAGE - Enforcement rights and method enforce rights in protected (secure) digital content available on a medium such as the Internet, an optical disk, etc.

DESCRIPTION OF DRAWING(S) - Drawing is a block diagram showing an enforcement architecture in accordance with an embodiment of the present invention.

Computing device 14

Digital licence 16

Black box 30

Decryption key. KD

CHOSEN-DRAWING: Dwg.1/22

TITLE-TERMS: DIGITAL MANAGEMENT SYSTEM OPERATE COMPUTATION DEVICE USER REQUEST  
ENCRYPTION DIGITAL CONTENT RENDER COMPUTER

DERWENT-CLASS: T01

EPI-CODES: T01-C01A; T01-D01; T01-H01B1; T01-H01C2; T01-H07C5E; T01-J12C;  
T01-J20B2A;

SECONDARY-ACC-NO:

Non-CPI Secondary Accession Numbers: N2001-368090

**WEST**☐ Generate Collection

L3: Entry 1 of 4

File: USPT

Jun 26, 2001

US-PAT-NO: 6253193

DOCUMENT-IDENTIFIER: US 6253193 B1

TITLE: Systems and methods for the secure transaction management and electronic rights protection

DATE-ISSUED: June 26, 2001

## INVENTOR-INFORMATION:

NAME	CITY	STATE	ZIP CODE	COUNTRY
Ginter; Karl L.	Beltsville	MD		
Shear; Victor H.	Bethesda	MD		
Spahn; Francis J.	El Cerrito	CA		
Van Wie; David M.	Sunnyvale	CA		

## ASSIGNEE-INFORMATION:

NAME	CITY	STATE	ZIP CODE	COUNTRY	TYPE	CODE
InterTrust Technologies Corporation	Santa Clara	CA				02

APPL-NO: 9/ 208017

DATE FILED: December 9, 1998

## PARENT-CASE:

This is a continuation of application Ser. No. 08/964,333, filed Nov. 4, 1997 now U.S. Pat. No. 5,982,891, which is a continuation of application Ser. No. 08/388,107, filed Feb. 13, 1995, now abandoned--all of which are incorporated herein by reference.

INT-CL: [7] H04L 9/32

US-CL-ISSUED: 705/57; 705/52

US-CL-CURRENT: 705/57; 705/52

FIELD-OF-SEARCH: 705/51, 705/52, 705/56, 705/57, 380/201-203, 386/94, 386/124

## PRIOR-ART-DISCLOSED:

## U.S. PATENT DOCUMENTS

☐ Search Selected☐ Search ALL

PAT-NO	ISSUE-DATE	PATENTEE-NAME	US-CL
<input type="checkbox"/> 3573747	April 1971	Adams et al.	N/A
<input type="checkbox"/> 3609697	September 1971	Blevins	N/A
<input type="checkbox"/> 3796830	March 1974	Smith	N/A
<input type="checkbox"/> 3798359	March 1974	Feistel	N/A
<input type="checkbox"/> 3798360	March 1974	Feistel	N/A
<input type="checkbox"/> 3798605	March 1974	Feistel	N/A

<input type="checkbox"/>	3806882	April 1974	Clarke	N/A
<input type="checkbox"/>	3829833	August 1974	Freeny	N/A
<input type="checkbox"/>	3906448	September 1975	Henriques	N/A
<input type="checkbox"/>	3911397	October 1975	Freeny	N/A
<input type="checkbox"/>	3924065	December 1975	Freeny	N/A
<input type="checkbox"/>	3931504	January 1976	Jacoby	N/A
<input type="checkbox"/>	3946220	March 1976	Brobeck et al.	N/A
<input type="checkbox"/>	3956615	May 1976	Anderson et al.	N/A
<input type="checkbox"/>	3958081	May 1976	Ehram et al.	N/A
<input type="checkbox"/>	3970992	July 1976	Boothroyd et al.	N/A
<input type="checkbox"/>	4048619	September 1977	Forman, Jr. et al.	N/A
<input type="checkbox"/>	4071911	January 1978	Mazur	N/A
<input type="checkbox"/>	4112421	September 1978	Freeny	N/A
<input type="checkbox"/>	4120030	October 1978	Johnstone	N/A
<input type="checkbox"/>	4163280	July 1979	Mori et al.	N/A
<input type="checkbox"/>	4168396	September 1979	Best	N/A
<input type="checkbox"/>	4196310	April 1980	Forman et al.	N/A
<input type="checkbox"/>	4200913	April 1980	Kuhar et al.	N/A
<input type="checkbox"/>	4209787	June 1980	Freeny	N/A
<input type="checkbox"/>	4217588	August 1980	Freeny	N/A
<input type="checkbox"/>	4220991	September 1980	Hamano et al.	N/A
<input type="checkbox"/>	4232193	November 1980	Gerard	N/A
<input type="checkbox"/>	4232317	November 1980	Freeny	N/A
<input type="checkbox"/>	4236217	November 1980	Kennedy	N/A
<input type="checkbox"/>	4253157	February 1981	Kirschner et al.	N/A
<input type="checkbox"/>	4262329	April 1981	Bright et al.	N/A
<input type="checkbox"/>	4265371	May 1981	Desai et al.	N/A
<input type="checkbox"/>	4270182	May 1981	Asija	N/A
<input type="checkbox"/>	4278837	July 1981	Best	N/A
<input type="checkbox"/>	4305131	December 1981	Best	N/A
<input type="checkbox"/>	4306289	December 1981	Lumley	N/A
<input type="checkbox"/>	4309569	January 1982	Merkle	N/A
<input type="checkbox"/>	4319079	March 1982	Best	N/A
<input type="checkbox"/>	4323921	April 1982	Guillou	N/A
<input type="checkbox"/>	4328544	May 1982	Baldwin et al.	N/A
<input type="checkbox"/>	4337483	June 1982	Guillou	N/A
<input type="checkbox"/>	4361877	November 1982	Dyer et al.	N/A
<input type="checkbox"/>	4375579	March 1983	Davida et al.	N/A

<input type="checkbox"/>	<u>4433207</u>	February 1984	Best	N/A
<input type="checkbox"/>	<u>4434464</u>	February 1984	Suzuki et al.	N/A
<input type="checkbox"/>	<u>4442486</u>	April 1984	Mayer	N/A
<input type="checkbox"/>	<u>4446519</u>	May 1984	Thomas	N/A
<input type="checkbox"/>	<u>4454594</u>	June 1984	Heffron et al.	N/A
<input type="checkbox"/>	<u>4458315</u>	July 1984	Uchenick	N/A
<input type="checkbox"/>	<u>4462076</u>	July 1984	Smith	N/A
<input type="checkbox"/>	<u>4462078</u>	July 1984	Ross	N/A
<input type="checkbox"/>	<u>4465901</u>	August 1984	Best	N/A
<input type="checkbox"/>	<u>4471163</u>	September 1984	Donald et al.	N/A
<input type="checkbox"/>	<u>4484217</u>	November 1984	Block et al.	N/A
<input type="checkbox"/>	<u>4494156</u>	January 1985	Kadison et al.	N/A
<input type="checkbox"/>	<u>4513174</u>	April 1985	Herman	N/A
<input type="checkbox"/>	<u>4528588</u>	July 1985	Lofberg	N/A
<input type="checkbox"/>	<u>4528643</u>	July 1985	Freeny	N/A
<input type="checkbox"/>	<u>4553252</u>	November 1985	Egendorf	N/A
<input type="checkbox"/>	<u>4558176</u>	December 1985	Arnold et al.	N/A
<input type="checkbox"/>	<u>4558413</u>	December 1985	Schmidt et al.	N/A
<input type="checkbox"/>	<u>4562306</u>	December 1985	Chou et al.	N/A
<input type="checkbox"/>	<u>4562495</u>	December 1985	Bond et al.	N/A
<input type="checkbox"/>	<u>4577289</u>	March 1986	Comerford et al.	N/A
<input type="checkbox"/>	<u>4584641</u>	April 1986	Guglielmino	N/A
<input type="checkbox"/>	<u>4588991</u>	May 1986	Atalla	N/A
<input type="checkbox"/>	<u>4589064</u>	May 1986	Chiba et al.	N/A
<input type="checkbox"/>	<u>4593353</u>	June 1986	Pickholtz	N/A
<input type="checkbox"/>	<u>4593376</u>	June 1986	Volk	N/A
<input type="checkbox"/>	<u>4595950</u>	June 1986	Lofberg	N/A
<input type="checkbox"/>	<u>4597058</u>	June 1986	Izumi et al.	N/A
<input type="checkbox"/>	<u>4634807</u>	January 1987	Chorley et al.	N/A
<input type="checkbox"/>	<u>4644493</u>	February 1987	Chandra et al.	N/A
<input type="checkbox"/>	<u>4646234</u>	February 1987	Tolman et al.	N/A
<input type="checkbox"/>	<u>4652990</u>	March 1987	Pailen et al.	N/A
<input type="checkbox"/>	<u>4658093</u>	April 1987	Hellman	N/A
<input type="checkbox"/>	<u>4670857</u>	June 1987	Rackman	N/A
<input type="checkbox"/>	<u>4672572</u>	June 1987	Alsberg	N/A
<input type="checkbox"/>	<u>4677434</u>	June 1987	Fascenda	N/A
<input type="checkbox"/>	<u>4680731</u>	July 1987	Izumi et al.	N/A
<input type="checkbox"/>	<u>4683553</u>	July 1987	Mollier	N/A

<input type="checkbox"/>	<u>4685056</u>	August 1987	Barnsdale et al.	N/A
<input type="checkbox"/>	<u>4688169</u>	August 1987	Joshi	N/A
<input type="checkbox"/>	<u>4691350</u>	September 1987	Kleijne et al.	N/A
<input type="checkbox"/>	<u>4696034</u>	September 1987	Wiedemer	N/A
<input type="checkbox"/>	<u>4700296</u>	October 1987	Palmer, Jr. et al.	705/32
<input type="checkbox"/>	<u>4701846</u>	October 1987	Ikeda et al.	N/A
<input type="checkbox"/>	<u>4712238</u>	December 1987	Gilhousen et al.	N/A
<input type="checkbox"/>	<u>4713753</u>	December 1987	Boebert et al.	N/A
<input type="checkbox"/>	<u>4740890</u>	April 1988	William	N/A
<input type="checkbox"/>	<u>4747139</u>	May 1988	Taaffe	N/A
<input type="checkbox"/>	<u>4757533</u>	July 1988	Allen et al.	N/A
<input type="checkbox"/>	<u>4757534</u>	July 1988	Matyas et al.	N/A
<input type="checkbox"/>	<u>4768087</u>	August 1988	Taub et al.	N/A
<input type="checkbox"/>	<u>4791565</u>	December 1988	Dunham et al.	N/A
<input type="checkbox"/>	<u>4796181</u>	January 1989	Wiedemer	N/A
<input type="checkbox"/>	<u>4799156</u>	January 1989	Shavit	N/A
<input type="checkbox"/>	<u>4807288</u>	February 1989	Ugon et al.	N/A
<input type="checkbox"/>	<u>4817140</u>	March 1989	Chandra et al.	N/A
<input type="checkbox"/>	<u>4823264</u>	April 1989	Deming	N/A
<input type="checkbox"/>	<u>4827508</u>	May 1989	Shear	N/A
<input type="checkbox"/>	<u>4858121</u>	August 1989	Barber et al.	N/A
<input type="checkbox"/>	<u>4864494</u>	September 1989	Kobus	N/A
<input type="checkbox"/>	<u>4866769</u>	September 1989	Karp	380/56
<input type="checkbox"/>	<u>4868877</u>	September 1989	Fischer	N/A
<input type="checkbox"/>	<u>4903296</u>	February 1990	Chandra et al.	N/A
<input type="checkbox"/>	<u>4924378</u>	May 1990	Hershey et al.	N/A
<input type="checkbox"/>	<u>4930073</u>	May 1990	Cina	N/A
<input type="checkbox"/>	<u>4949187</u>	August 1990	Cohen	N/A
<input type="checkbox"/>	<u>4975647</u>	December 1990	Downer et al.	713/168
<input type="checkbox"/>	<u>4977594</u>	December 1990	Shear	N/A
<input type="checkbox"/>	<u>4999806</u>	March 1991	Chernow et al.	N/A
<input type="checkbox"/>	<u>5001752</u>	March 1991	Fischer	N/A
<input type="checkbox"/>	<u>5005122</u>	April 1991	Griffin et al.	N/A
<input type="checkbox"/>	<u>5005200</u>	April 1991	Fischer	N/A
<input type="checkbox"/>	<u>5010571</u>	April 1991	Katznelson	N/A
<input type="checkbox"/>	<u>5023907</u>	June 1991	Johnson et al.	N/A
<input type="checkbox"/>	<u>5047928</u>	September 1991	Wiedemer	N/A
<input type="checkbox"/>	<u>5048085</u>	September 1991	Abraham et al.	N/A

<input type="checkbox"/>	<u>5050213</u>	September 1991	Shear	N/A
<input type="checkbox"/>	<u>5091966</u>	February 1992	Bloomberg et al.	N/A
<input type="checkbox"/>	<u>5103392</u>	April 1992	Mori et al.	N/A
<input type="checkbox"/>	<u>5103476</u>	April 1992	Waite et al.	N/A
<input type="checkbox"/>	<u>5111390</u>	May 1992	Ketcham	N/A
<input type="checkbox"/>	<u>5119493</u>	June 1992	Janis et al.	N/A
<input type="checkbox"/>	<u>5128525</u>	July 1992	Stearns et al.	N/A
<input type="checkbox"/>	<u>5136643</u>	August 1992	Fischer	N/A
<input type="checkbox"/>	<u>5136646</u>	August 1992	Haber	N/A
<input type="checkbox"/>	<u>5136647</u>	August 1992	Haber	N/A
<input type="checkbox"/>	<u>5136716</u>	August 1992	Harvey et al.	N/A
<input type="checkbox"/>	<u>5146575</u>	September 1992	Nolan	N/A
<input type="checkbox"/>	<u>5148481</u>	September 1992	Abraham et al.	N/A
<input type="checkbox"/>	<u>5155680</u>	October 1992	Wiedemer	N/A
<input type="checkbox"/>	<u>5163091</u>	November 1992	Graziano et al.	N/A
<input type="checkbox"/>	<u>5168147</u>	December 1992	Bloomberg	N/A
<input type="checkbox"/>	<u>5185717</u>	February 1993	Mori	N/A
<input type="checkbox"/>	<u>5201046</u>	April 1993	Goldberg et al.	N/A
<input type="checkbox"/>	<u>5201047</u>	April 1993	Maki et al.	N/A
<input type="checkbox"/>	<u>5208748</u>	May 1993	Flores et al.	N/A
<input type="checkbox"/>	<u>5214702</u>	May 1993	Fischer	N/A
<input type="checkbox"/>	<u>5216603</u>	June 1993	Flores et al.	N/A
<input type="checkbox"/>	<u>5221833</u>	June 1993	Hecht	N/A
<input type="checkbox"/>	<u>5222134</u>	June 1993	Waite et al.	N/A
<input type="checkbox"/>	<u>5224160</u>	June 1993	Paulini et al.	N/A
<input type="checkbox"/>	<u>5224163</u>	June 1993	Gasser et al.	N/A
<input type="checkbox"/>	<u>5235642</u>	August 1993	Wobber et al.	N/A
<input type="checkbox"/>	<u>5245165</u>	September 1993	Zhang	N/A
<input type="checkbox"/>	<u>5247575</u>	September 1993	Sprague et al.	N/A
<input type="checkbox"/>	<u>5260999</u>	November 1993	Wyman	N/A
<input type="checkbox"/>	<u>5263158</u>	November 1993	Janis	N/A
<input type="checkbox"/>	<u>5265164</u>	November 1993	Matyas et al.	N/A
<input type="checkbox"/>	<u>5276735</u>	January 1994	Boebert et al.	N/A
<input type="checkbox"/>	<u>5280479</u>	January 1994	Mary	N/A
<input type="checkbox"/>	<u>5285494</u>	February 1994	Sprecher et al.	N/A
<input type="checkbox"/>	<u>5301231</u>	April 1994	Abraham et al.	N/A
<input type="checkbox"/>	<u>5311591</u>	May 1994	Fischer	N/A
<input type="checkbox"/>	<u>5319705</u>	June 1994	Halter et al.	N/A

<input type="checkbox"/>	5319785	June 1994	Halter et al.	N/A
<input type="checkbox"/>	5337360	August 1994	Fischer	N/A
<input type="checkbox"/>	5341429	August 1994	Stringer et al.	N/A
<input type="checkbox"/>	5343527	August 1994	Moore et al.	N/A
<input type="checkbox"/>	5347579	September 1994	Blandford	N/A
<input type="checkbox"/>	5351293	September 1994	Michener	N/A
<input type="checkbox"/>	5355474	October 1994	Thuraisingham et al.	N/A
<input type="checkbox"/>	5373561	December 1994	Haber et al.	N/A
<input type="checkbox"/>	5390247	February 1995	Fischer	N/A
<input type="checkbox"/>	5390330	February 1995	Talati	N/A
<input type="checkbox"/>	5392220	February 1995	van der Hamer et al.	N/A
<input type="checkbox"/>	5392390	February 1995	Crozier	N/A
<input type="checkbox"/>	5394469	February 1995	Nagel et al.	N/A
<input type="checkbox"/>	5410598	April 1995	Shear	N/A
<input type="checkbox"/>	5412717	May 1995	Fischer	N/A
<input type="checkbox"/>	5421006	May 1995	Jablon	N/A
<input type="checkbox"/>	5422953	June 1995	Fischer	N/A
<input type="checkbox"/>	5428606	June 1995	Moskowitz	N/A
<input type="checkbox"/>	5438508	August 1995	Wyman	N/A
<input type="checkbox"/>	5442645	August 1995	Ugon	N/A
<input type="checkbox"/>	5444779	August 1995	Daniele	N/A
<input type="checkbox"/>	5449895	September 1995	Hecht et al.	N/A
<input type="checkbox"/>	5449896	September 1995	Hecht et al.	N/A
<input type="checkbox"/>	5450493	September 1995	Maher	N/A
<input type="checkbox"/>	5453601	September 1995	Rosen	N/A
<input type="checkbox"/>	5453605	September 1995	Hecht et al.	N/A
<input type="checkbox"/>	5455407	October 1995	Rosen	N/A
<input type="checkbox"/>	5455861	October 1995	Faucher et al.	N/A
<input type="checkbox"/>	5455953	October 1995	Russell	N/A
<input type="checkbox"/>	5457746	October 1995	Dolphin	N/A
<input type="checkbox"/>	5463565	October 1995	Cookson et al.	N/A
<input type="checkbox"/>	5473687	December 1995	Lipscomb et al.	N/A
<input type="checkbox"/>	5473692	December 1995	Davis	N/A
<input type="checkbox"/>	5479509	December 1995	Ugon	N/A
<input type="checkbox"/>	5485622	January 1996	Yamaki	N/A
<input type="checkbox"/>	5491800	February 1996	Goldsmith et al.	N/A
<input type="checkbox"/>	5497479	March 1996	Hornbuckle	N/A
<input type="checkbox"/>	5497491	March 1996	Mitchell et al.	N/A

<input type="checkbox"/>	5499298	March 1996	Narasimhalu et al.	N/A
<input type="checkbox"/>	5504757	April 1996	Cook et al.	N/A
<input type="checkbox"/>	5504818	April 1996	Okano	N/A
<input type="checkbox"/>	5504837	April 1996	Griffeth et al.	N/A
<input type="checkbox"/>	5508913	April 1996	Yamamoto et al.	N/A
<input type="checkbox"/>	5509070	April 1996	Schull	N/A
<input type="checkbox"/>	5513261	April 1996	Maher	N/A
<input type="checkbox"/>	5517518	May 1996	Rosen	N/A
<input type="checkbox"/>	5530235	June 1996	Stefik et al.	N/A
<input type="checkbox"/>	5530752	June 1996	Rubin	N/A
<input type="checkbox"/>	5533123	July 1996	Force et al.	N/A
<input type="checkbox"/>	5534975	July 1996	Stefik et al.	N/A
<input type="checkbox"/>	5537526	July 1996	Anderson et al.	N/A
<input type="checkbox"/>	5539735	July 1996	Moskowitz	N/A
<input type="checkbox"/>	5539828	July 1996	Davis	N/A
<input type="checkbox"/>	5550971	August 1996	Brunner et al.	N/A
<input type="checkbox"/>	5553282	September 1996	Parrish et al.	N/A
<input type="checkbox"/>	5557518	September 1996	Rosen	N/A
<input type="checkbox"/>	5563946	October 1996	Cooper et al.	N/A
<input type="checkbox"/>	5568552	October 1996	Davis	N/A
<input type="checkbox"/>	5572673	November 1996	Shurts	N/A
<input type="checkbox"/>	5592549	January 1997	Nagel et al.	N/A
<input type="checkbox"/>	5606609	February 1997	Houser et al.	N/A
<input type="checkbox"/>	5613004	March 1997	Cooperman et al.	N/A
<input type="checkbox"/>	5621797	April 1997	Rosen	N/A
<input type="checkbox"/>	5629980	May 1997	Stefik et al.	N/A
<input type="checkbox"/>	5633932	May 1997	Davis	N/A
<input type="checkbox"/>	5634012	May 1997	Stefik et al.	N/A
<input type="checkbox"/>	5636292	June 1997	Rhoads	N/A
<input type="checkbox"/>	5638443	June 1997	Stefik	N/A
<input type="checkbox"/>	5638504	June 1997	Scott et al.	N/A
<input type="checkbox"/>	5640546	June 1997	Gopinath	N/A
<input type="checkbox"/>	5655077	August 1997	Jones et al.	N/A
<input type="checkbox"/>	5687236	November 1997	Moskowitz et al.	N/A
<input type="checkbox"/>	5689587	November 1997	Bender	N/A
<input type="checkbox"/>	5692180	November 1997	Lee	N/A
<input type="checkbox"/>	5710834	January 1998	Rhoads	N/A
<input type="checkbox"/>	5740549	April 1998	Reilly et al.	N/A

<input type="checkbox"/> 5745604	April 1998	Rhoads	N/A
<input type="checkbox"/> 5748763	May 1998	Rhoads	N/A
<input type="checkbox"/> 5748783	May 1998	Rhoads	N/A
<input type="checkbox"/> 5754849	May 1998	Dyer et al.	N/A
<input type="checkbox"/> 5758152	May 1998	LeTourneau	N/A
<input type="checkbox"/> 5765152	June 1998	Erickson	N/A
<input type="checkbox"/> 5768426	June 1998	Rhoads	N/A

## FOREIGN PATENT DOCUMENTS

FOREIGN-PAT-NO	PUBN-DATE	COUNTRY	US-CL
62-241061	December 1984	BEX	
9 004 79	December 1984	BEX	
3803982A1	January 1990	DEX	
0 084 441 A1	July 1983	EPX	
0 128 672 A1	December 1984	EPX	
0 135 422 A1	March 1985	EPX	
0 180 460 A1	May 1986	EPX	
0 370 146 A1	May 1990	EPX	
0 399 822 A2	November 1990	EPX	
0 421 409 A2	April 1991	EPX	
0 456 386 A2	November 1991	EPX	
0 469 864 A3	February 1992	EPX	
0 469 864 A2	February 1992	EPX	
0 565 314 A2	October 1993	EPX	
0 593 305 A2	April 1994	EPX	
0 651 554 A1	May 1995	EPX	
0 668 695 A2	August 1995	EPX	
0 668 695 A3	August 1995	EPX	
0 725 376 A2	January 1996	EPX	
0 695 985 A1	February 1996	EPX	
0 696 798 A1	February 1996	EPX	
0 715 243 A1	June 1996	EPX	
0 715 244 A1	June 1996	EPX	
0 715 245 A1	June 1996	EPX	
0 715 246 A1	June 1996	EPX	
2136175	September 1984	GBX	
2264796A	September 1993	GBX	
2294348	April 1996	GBX	
2295947	June 1996	GBX	
57-726	May 1982	JPX	
62-225059	August 1987	JPX	
62-241061	October 1987	JPX	
1-068835	March 1989	JPX	
64-68835	March 1989	JPX	
2-242352	September 1990	JPX	
2-247763	October 1990	JPX	
2-294855	December 1990	JPX	
4-369068	December 1992	JPX	
5-181734	July 1993	JPX	

5-257783	October 1993	JPX
5-268415	October 1993	JPX
6-175794	June 1994	JPX
6-215010	August 1994	JPX
7-056794	March 1995	JPX
7-084852	March 1995	JPX
7-141138	June 1995	JPX
7-200317	August 1995	JPX
7-200492	August 1995	JPX
7-244639	September 1995	JPX
8-137795	May 1996	JPX
8-152990	June 1996	JPX
8-185292	July 1996	JPX
8-105298	July 1996	JPX
WO 85/02310	May 1985	WOX
WO 85/03584	August 1985	WOX
WO 90/02382	March 1990	WOX
WO 92/06438	April 1992	WOX
WO 92/22870	December 1992	WOX
WO 93/01550	January 1993	WOX
WO 94/01821	January 1994	WOX
WO 94/03859	February 1994	WOX
WO 94/06103	March 1994	WOX
WO 94/16395	July 1994	WOX
WO 94/18620	August 1994	WOX
WO 94/22266	September 1994	WOX
WO 94/27406	November 1994	WOX
WO 95/14289	May 1995	WOX
WO 96/00963	January 1996	WOX
WO 96/06503	February 1996	WOX
WO 96/03835	February 1996	WOX
WO 96/05698	February 1996	WOX
WO 96/13013	May 1996	WOX
WO 96/21192	July 1996	WOX
WO 96/24092	August 1996	WOX
WO 97/03423	January 1997	WOX
WO 97/07656	March 1997	WOX
WO 97/32251	September 1997	WOX
WO 97/48203	December 1997	WOX

## OTHER PUBLICATIONS

David Arneke and Donna Cunningham, Document from the Internet: AT&T encryption system protects information services, (News Release), Jan. 9, 1995, 1 page.

Claude Baggett, Cable's Emerging Role in the Information Superhighway, Cable Labs, (undated) 13 slides.

Theodore Sedgwick Barassi, Document from Internet: The Cybernotary: Public Key Registration and Certification and Authentication of International Legal Transactions, (undated), 4 pages.

Hugh Barnes, e-mail to Henry LaMuth, subject: George Gilder articles, May 31, 1994, 2 pages.

Comments in the Matter of Public Hearing and Request for Comments on the International Aspects of the National Information Infrastructure, Before the Department of Commerce, Aug. 12, 1994, pp. 1-15 (comments of Dan Bart).

Michael Baum, "Worldwide Electronic Commerce: Law, Policy and Controls Conference," program details, Nov. 11, 1993, 18 pages.

Robert M. Best, Preventing Software Piracy With Crypto-Microprocessors, Digest

of Papers, VLSI: New Architectural Horizons, Feb. 1980, pp. 466-469.

Richard L. Bisbey, II and Gerald J Popek, Encapsulation: An Approach to Operating System Security, (USC/Information Science Institute, Marina Del Rey, CA) Oct. 1973, pp. 666-675.

Rolf Blom, Robert Forchheimer, et al. Encryption Methods in Data Networks, Ericsson Technics, No. 2, Stockholm, Sweden, 1978.

Rick E. Bruner, Document from the Internet: PowerAgent, NetBot help advertisers reach Internet shoppers, Aug. 1997, 3 pages.

Denise Caruso, Technology, Digital Commerce: 2 plans for watermarks, which can bind proof of authorship to electronic works., N.Y. Times, Aug. 7, 1995, p. D5.

A.K. Choudhury, N. F. Maxemchuck, et al., Copyright Protection for Electronic Publishing Over Computer Networks, (AT&T Bell Laboratories, Murray Hill N. J.) Jun. 1994, 17 pages.

Tim Clark, Ad service gives cash back, (visited Aug. 4, 1997) 2 pages.

Donna Cunningham, David Arneke, et al., Document from the Internet: AT&T, VLSI Technology join to improve info highway security, (News Release) Jan., 31, 1995, 3 pages.

Lorcan Dempsey and Stuart Weibel, The Warwick Metadata Workshop: A Framework for the Deployment of Resource Description, D-Lib Magazine, Jul., 15, 1996.

Dorothy E. Denning and Peter J Denning, Data Security, 11 Computing Surveys No. 3, Sep. 1979, pp. 227-249.

Whitfield Diffie and Martin E. Hellman, New Directions in Cryptography, IEEE Transactions on Information Theory, vol. 22, No. 6, Nov. 1976, pp. 644-651.

Whitfield Diffie and Martin E. Hellman, Privacy and Authentication: An Introduction to Cryptography, Proceedings of the IEEE, vol. 67, No. 3, Mar. 1979 pp. 397-427.

Stephen R. Dusse and Burton S. Kaliski, A Cryptographic Library for the Motorola 56000,, Advances in Cryptology-Proceedings Eurocrypt 90, (I.M. Damgard, ed., Springer-Verlag) 1991, pp. 230-244.

Esther Dyson, Intellectual Value, Wired Magazine, Jul. 1995, pp. 136-141 and 182-183 (This article is not prior art.).

Science, space and technology, Hearing before Subcomm. on Technology, Environment, ad Aviation, May 26, 1994 (testimony of D. Linda Garcia).

James Gleick, Dead as a Dollar, The New York Times Magazine, Jun. 16, 1996, Sect. 6, pp. 26-30, 35, 42, 50, 54.

Fred Greguras, Document from Internet: Softic Symposium '95, Copyright Clearances and Moral Rights, Dec. 11, 1995, 3 pages.

Louis C. Guillou, Smart Cards and Conditional Access, Advances in Cryptography--Proceedings of EuroCrypt 84 (T. Beth et al, Ed., Springer-Verlag) 1985, pp. 480-490.

Harry H. Harman, Modern Factor Analysis, Third Edition Revised, University of Chicago Press, Chicago and London, 1976.

Amir Herzberg and Shlomit S. Pinter, Public Protection of Software, ACM Transactions on Computer Systems, vol. 5, No. 4, Nov. 1987, pp. 371-393.

Jud Hofmann, Interfacing the NII to User Homes, (Consumer Electronic Bus Committee) NIST, Jul. 1994, 12 slides.

Jud Hofmann, Interfacing the NII to User Homes, Electronic Industries Association, (Consumer Electronic Bus Committee) (undated), 14 slides.

Stannie Holt, Document from the Internet: Start-up promises user confidentiality in Web marketing service, InfoWorld Electric News (updated Aug. 13, 1997).

Jay J. Jiang and David W. Conrath, A concept-based Approach to Retrieval from an Electronic Industrial Directory, International Journal of Electronic Commerce, vol. 1, No. 1 (fall 1966) pp. 51-72.

Debra Jones, Document from the Internet: Top Tech Stories, PowerAgent Introduces First Internet `Informediary` to Empower and Protect Consumers, (updated Aug. 13, 1997) 3 pages.

Kevin Kelly, E-Money, Whole Earth Review, Summer 1993,, pp. 40-59.

Stephen Thomas Kent, Protecting Externally Supplied Software in Small Computers, (MIT/LCS/TR-255) Sep. 1980 254 pages.

David M. Kristol, Steven H. Low and Nicholas F. Maxemchuk, Anonymous Internet Mercantile Protocol, (AT&T Bell Laboratories, Murray Hill, NJ) Draft: Mar. 17, 1994.

Carl Lagoze, The Warwick Framework, A Container Architecture for Diverse Sets of Metadata, D-Lib Magazine, Jul./Aug. 1996.

Mike Lanza, e-mail, George Gilder's Fifth Article--Digital Darkhorse--Newspapers, Feb. 21, 1994.

Steven Levy, E-Money, That's What I want, Wired, Dec. 1994, 10 pages.

Steven H. Low and Nicholas F. Maxemchuk, Anonymous Credit Cards, AT&T Bell Laboratories, Proceedings of the 2<sup>sup</sup>.nd ACM Conference on Computer and Communication Security, Fairfax, Virginia, Nov. 2-4, 1994, 10 pages.

Steven H. Low, Nicholas F. Maxemchuk, and Sanjoy Paul, Anonymous Credit Cards and its Collusion Analysis (AT&T Bell Laboratories, Murray Hill, N.J.) Oct. 10, 1994, 18 pages.

S. H. Low, N.F. Maxemchuk, et al., Document Marking and Identification using both Line and word Shifting (AT&T Bell Laboratories, Murray Hill, N.J.) Jul. 29, 1994, 22 pages.

Malcolm MacLachlan, Document from the Internet: PowerAgent Debuts Spam-Free Marketing, TechWire, Aug. 13 1997, 3 pages.

N. F. Maxemchuk, Electronic Document Distribution, (AT&T Bell Laboratories, Murray Hill, N.J.) (undated).

Eric Milbrandt, Document from the Internet: Steganography Info and Archive, 1996, 2 pages.

Ryoichi Mori and Masaji Kawahara, Superdistribution: The concept and the Architecture, The Transactions of The EIEICE, V, E73 No. 7, Tokyo, Japan, Jul. 1990.

Walter S. Mossberg, Personal Technology, Threats to Privacy On-Line Become More Worrisome, The Wall Street Journal, Oct. 24, 1996.

Nicholas Negroponte, Some Thoughts on Likely and expected Communications scenarios: A Rebuttal, Telecommunications, Jan. 1993, pp. 41-42.

Nicholas Negroponte, Electronic Word of Mouth, Wired, Oct. 1996, p. 218.

Peter G. Neumann, Robert S. Boyer, et al., A Provably Secure Operating System: The System, Its Applications, and Proofs, Computer Science Laboratory Report CSL-116, Second Edition, SRI International, Jun. 1980.

Joseph N Pelton (Dr.), Why Nicholas Negroponte is Wrong About the Future of Telecommunication, Telecommunications, Jan. 1993, pp. 35-40.

Gordon Rankine (Dr.), Thomas--A Complete Single-Chip RSA Device, Advances in Cryptography, Proceedings of CRYPTO 86, (A.M. Odizko Ed., Springer-Verlag) 1987, pp. 480-487.

Arthur K. Reilly, Input to the `International Telecommunications Hearings,` Panel 1: Component Technologies of the NII/GII, Standards committee T1-Telecommunications (undated).

Paul Resnick and Hal R. Varion, Recommender Systems, Communications of the ACM, vol. 40, No. 3, Mar. 1997 pp. 56-89.

Lance Rose, Cyberspace and the Legal Matrix: Laws or Confusion?, 1991.

Steve Rosenthal, Interactive Network: Viewers Get Involved, New Media, Dec. 1992, pp. 30-31.

Steve Rosenthal, Interactive TV: The Gold Rush is on, New Media, Dec. 1992, pp. 27-29.

Steve Rosenthal, Mega Channels, New Media, Sep. 1993, pp. 36-46.

Edward Rothstein, Technology, Connections, Making the Internet come to you through `push` technology, N. Y. Times, Jan. 20, 1997, p. D5.

Ken Rutkowski, Document from Internet: PowerAgent Introduces First Internet `Informediary` to Empower and Protect Consumers, Tech Talk News Story, Aug. 4, 1997, 1 page.

Ira Sager (Edited by), Bits & Bytes, Business Week, Sep. 23, 1996, p. 142E.

Schlossstein, Steven, America: The G7's Comeback Kid, International Economy, Jun./Jul. 1993, 5 pages.

Ingrid Schnaumüller-Bichl and Ernst Piller, A Method of Software Protection Based on the Use of Smart Cards and Cryptographic Techniques, (no date), 9 pages.

Jurgen Schurmann, Pattern Classification, A Unified View of Statistical and Neural Approaches, John Wiley & Sons, Inc., 1996.

Victor Shear, Solutions for CD-ROM Pricing and Data Security Problems, CD ROM Yearbook 1988-1989 (Microsoft Press 1988 or 1989) pp. 530-533.

Karl Siuda, Security Services in Telecommunications Networks, Seminar: Mapping New Applications Onto New Technologies, edited by B. Plattner and P Gunzburger; Zurich, Mar. 8-10, 1988, pp. 45-52, XPO00215989.

Sean Smith and J.D. Tygar, Signed Vector Timestamps: A Secure Protocol for Partial Order Time, CMU-93-116, School of Computer Science Carnegie Mellon University, Pittsburgh, Pennsylvania, Oct. 1991; version of Feb. 1993, 15 pages.

Mark Stefik, Letting Loose the Light: Igniting Commerce in Electronic Publication, (Xerox PARC, Palo Alto, CA) 1994-1995, 35 pages.

Mark Stefik, Letting Loose the Light: Igniting Commerce In Electronic Publication, Internet Dreams: Archetypes, Myths, and Metaphors. Massachusetts Institute of Technology, 1996, pp. 219-253.

Mark Stefik, Chapter 7, Classification Introduction to Knowledge Systems. Morgan Kaufmann Publishers, Inc. 1995, pp. 543-607.

Tom Stephenson, The Info Infrastructure Initiative: Data Super Highways and You, Advanced Imaging. May 1993, pp. 73-74.

Bruce Sterling, Literary freeware: Not for Commercial Use, remarks at Computers, Freedom and Private Conference IV, Chicago, IL Mar. 26, 1994.

Bruno Struif, The Use of Chipcards for Electronic Signatures and encryption, Proceedings for the 1989 Conference on VSLI and Computer Peripherals, Computer Society Press, 1989, pp. (4)155-(4)158.

J.D. Tygar and Bennet Yee, Cryptography: It's Not Just For Electronic Mail Anymore, CMU-CS-93-107, School of Computer Science Carnegie Mellon University, Pittsburgh, PA, Mar. 1, 1993, 21 pages.

J.D. Tygar and Bennet Yee, Dyad: A System for Using Physically Secure Coprocessors, School of Computer Science, Carnegie Mellon University, Pittsburgh, PA (undated), 41 pages.

J.D. Tygar and Bennet Yee, Dyad: A System for Using Physically Secure Coprocessors, School of Computer Science, Carnegie Mellon University, Pittsburgh, PA, May 1991, 36 pages.

T. Valovic, The Role of Computer Networking in the Emerging Virtual Marketplace, Telecommunications, (undated), pp. 40-44.

Joan Voight, Beyond the Banner, Wired, Dec. 1996, pp. 196, 200, 204.

Steven Vonder Haar, Document from the Internet: PowerAgent Launches Commercial Service, Interactive Week, Aug. 4, 1997, 1 page.

Robert Weber, Metering Technologies for Digital Intellectual Property, A Report to the International Federation of Reproduction Rights Organisations (Boston, MA), Oct. 1994, pp. 1-29.

Robert Weber, Document from the Internet: Digital Rights Management Technologies, Oct. 1995, 21 pages.

Robert Weber, Digital Rights Management Technologies, A Report to the International Federation of Reproduction Rights Organisations, Northeast Consulting Resources, Inc., Oct. 1995, 49 pages.

Adele Weder, Life on the Infohighway, INSITE, (no date), pp. 23-25.

Steve H. Weingart, Physical Security for the Abyss System, (IBM Thomas J. Watson Research Center, Yorktown Heights, NY), 1987, pp. 52-58.

Daniel J Weitzner, A Statement of EFF's Open Platform Campaign as of Nov., 1993, 3 pages.

Steve R. White, Abyss: A Trusted Architecture for Software Protection, (IBM Thomas J. Watson Research Center, Yorktown Heights, NY), 1987, pp. 38-50.

Bennet Yee, Using Secure Coprocessors, CMU-CS-94-149, School of Computer Science, Carnegie Mellon University, Pittsburgh, PA, 1994, 94 pages.

Frank Yellin, Document from the Internet: Low Level Security in Java, Sun Microsystems, 1996, 8 pages.

Symposium: Applications Requirements for Innovative video Programming; How to Foster (or Cripple) Program Development Opportunities for Interactive Video Programs Delivered on Optical Media: A Challenge for the Introduction of DVD (Digital Video Disc) (Oct 19-20, 1995, Sheraton Universal Hotel, Universal City CA).

Argent Information, Q&A Sheet Copyright 1995, The Dice Company, (last modified Jun. 16, 1996), 7 pages.

New Products, Systems and Services, AT&T Technology, vol. 9, No. 4, (undated), pp. 16-19.

Cable Television and America's Telecommunications Infrastructure, (National Cable Television Association, Washington, D.C.), Apr. 1993, 19 pages.

CD ROM: Introducing . . . The Workflow CD-ROM Sampler (Creative Networks, MCIMail: Creative Networks, Inc.), (no date).

Codercard, Basic Coder Subsystem (Interstate Electronics Corp., Anaheim, C.A.), (no date) 4 pages.

Collection of documents including: Protecting Electronically Published Properties, Increasing Publishing Profits, (Electronic Publishing Resources Inc., ) Jan. 1993, 25 pages.

Communications of the ACM, vol. 39, No. 6, Jun. 1996, 130 pages.

Communications of the ACM, "Intelligent Agents," vol. 37, No. 7 Jul. 1994, 170 pages.

Computer Systems Policy Project (CSSP), Perspectives on the National Information Infrastructure: Ensuring Interoperability, Feb. 1994, 5 slides.

DiscStore (Electronic Publishing Resources, Chevy Chase, M.D.), 1991.

DSP56000/DSP56001 Digital Signal Processors User's Manual, (Motorola), 1990, pp. 2-2.

A Supplement to Midrange Systems, Premenos Corp. White Paper: The Future of

Electronics Commerce, Document from Internet, (Premenos) Aug. 1995, 4 pages.  
CGI Common Gateway Interface Document from the Internet, , 1996, 1 page.  
HotJava.TM.: The Security Story Document from the Internet, (no date) 4 pages.  
About the Digital Notary Service Document from Internet, (Surety Technologies), 1994-5, 6 pages.  
Templar Software and Services, Secure, Reliable, Standards-Based EDI Over the Internet, Document from Internet, (Premenos) (no date), 1 page.  
Javasoft, Frequently Asked Questions--Applet Security, Document from Internet, Jun. 7, 1996, 8 pages.  
News from The Document Company Xerox, Xerox Announces Software Kit for Creating `Working Documents` with Dataglyphs Document from Internet, Nov. 6, 1995, 13 pages.  
Premenos Announces Templar 2.0--Next Generation Software for Secure Internet EDI, Document from Internet, Jan. 17, 1996, 1 page.  
WEPIN Store, Stenography (Hidden Writing), Document from Internet, (Common Law), 1995, 1 page.  
Sag's durch die Blume, Document from Internet, (German), (no date), 5 pages.  
A Publication of the Electronic Frontier Foundation, EFFector Online vol. 6 No. 6., Dec. 6, 1993, 8 pages.  
EIA and TIA White Paper on National Information Infrastructure, The Electronic Industries Association and the Telecommunications Industry Association, Washington, D.C., (no date).  
Electronic Currency Requirements, XIWT (Cross Industry Working Group), (no date).  
Electronic Publishing Resources Inc. Protecting Electronically Published Properties Increasing Publishing Profits (Electronic Publishing Resources, Chevy Chase, MD) 1991, 19 pages.  
What is Firefly?, www.ffly.com, (Firefly Network, Inc.) Firefly revision: 41.4, (Copyright 1995), 1996, 1 page.  
First CII Honeywell Bull International Symposium on Computer Security and Confidentiality, conference Text Jan. 26-28, 1981, pp. 1-21.  
Framework for National Information Infrastructure Services, Draft, U.S. Department of Commerce, Jul. 1994.  
Framework for National Information Infrastructure Services, Jul. 1994, 12 Slides.  
Intellectual Property and the National Information Infrastructure, a Preliminary Draft of the Report of the Working Group on Intellectual Property Rights, Green paper, Jul. 1994, 141 pages.  
Multimedia Mixed Objects Envelopes Supporting a Graduated Fee Scheme Via Encryption, IBM Technical Disclosure Bulletin, vol. 37, No. 3, Mar. 1, 1994, pp. 413-417, XP000441522.  
Transformer Rules Strategy for Software Distribution Mechanism-Support Products, IBM Technical Disclosure Bulletin, vol. 37, No. 48, Apr. 1994, pp. 523-525, XP000451335.  
IISP Break Out Session Report for Group Number 3, Standards Development and Tracking System, (no date).  
Information Infrastructure Standards Panel: NII "The Information Superhighway", NationsBank--HGDeal--ASC X9, (no date), 15 pages.  
Invoice? What's an Invoice?, Business Week, Jun. 10, 1996, pp. 110-112.  
Micro Card (Micro Card Technologies, Inc., Dallas, TX), (no date), 4 pages.  
Background on the Administration's Telecommunications Policy Reform Initiative, News Release, The White House, Office of the President, Jan. 11, 1994, 7 pages.

NII, Architecture Requirements, XIWT, (no date).  
Symposium: Open System Environment Architectural Framework for National Information Infrastructure Services and Standards, in Support of National Class Distributed Systems, Distributed System Engineering Program Sponsor Group, Draft 1.0, Aug. 5, 1994, 34 pages.  
Proper Use of Consumer Information on the Internet, Document from the Internet, White Paper, (PowerAgent Inc., Melo Park, CA) Jun 1997, 9 pages.  
What the Experts are Reporting on Power Agent, Document from the Internet, PowerAgent Press Releases, Aug. 13, 1997, 6 pages.  
What the Experts are Reporting on PowerAgent, Document from the Internet, PowerAgent Press Releases, Aug. 4, 1997, 5 pages.  
What the Experts are Reporting on PowerAgent, Document from the Internet, PowerAgent Press Releases, Aug. 13, 1997, 3 pages.

ART-UNIT: 277

PRIMARY-EXAMINER: Barron, Jr.; Gilberto

ATTY-AGENT-FIRM: Finnegan, Henderson, Farabow, Garrett & Dunner L.L.P.

ABSTRACT:

The present invention provides systems and methods for secure transaction management and electronic rights protection. Electronic appliances such as computers equipped in accordance with the present invention help to ensure that information is accessed and used only in authorized ways, and maintain the integrity, availability, and/or confidentiality of the information. Such electronic appliances provide a distributed virtual distribution environment (VDE) that may enforce a secure chain of handling and control, for example, to control and/or meter or otherwise monitor use of electronically stored or disseminated information. Such a virtual distribution environment may be used to protect rights of various participants in electronic commerce and other electronic or electronic-facilitated transactions. Distributed and other operating systems, environments and architectures, such as, for example, those using tamper-resistant hardware-based processors, may establish security at each node. These techniques may be used to support an all-electronic information distribution, for example, utilizing the "electronic highway."

72 Claims, 155 Drawing figures

**WEST****End of Result Set****Generate Collection**

L3: Entry 4 of 4

File: USPT

Feb 3, 1998

US-PAT-NO: 5715403

DOCUMENT-IDENTIFIER: US 5715403 A

TITLE: System for controlling the distribution and use of digital works having attached usage rights where the usage rights are defined by a usage rights grammar

DATE-ISSUED: February 3, 1998

## INVENTOR-INFORMATION:

NAME	CITY	STATE	ZIP CODE	COUNTRY
Stefik; Mark J.	Woodside	CA		

## ASSIGNEE-INFORMATION:

NAME	CITY	STATE	ZIP CODE	COUNTRY	TYPE CODE
Xerox Corporation	Stamford	CT			02

APPL-NO: 8/ 344041

DATE FILED: November 23, 1994

INT-CL: [6] G06F 1/14, G06F 13/372

US-CL-ISSUED: 395/244; 395/188.01, 395/800, 380/23

US-CL-CURRENT: 705/44; 705/54, 705/57, 709/229, 713/202

FIELD-OF-SEARCH: 395/800, 395/600, 395/700, 395/775, 395/650, 395/182.13, 395/608, 395/183.14, 395/201, 395/569, 395/825, 395/712, 395/187.01, 395/188.01, 395/244, 395/217, 380/4, 380/15, 380/18, 380/20, 380/25, 380/24, 380/23, 380/30, 364/DIG.1, 364/DIG.2, 364/41R, 340/825.33, 340/825.34, 348/3, 455/4.1, 455/5.1, 455/26.1

PRIOR-ART-DISCLOSED:

U.S. PATENT DOCUMENTS

**Search Selected****Search ALL**

PAT-NO	ISSUE-DATE	PATENTEE-NAME	US-CL
<input type="checkbox"/> 3790700	February 1974	Callais et al.	348/3
<input type="checkbox"/> 4529870	July 1985	Chaum	235/380
<input type="checkbox"/> 4658093	April 1987	Hellman	380/25
<input type="checkbox"/> 4891838	January 1990	Faber	380/25
<input type="checkbox"/> 4924378	May 1990	Hershey et al.	364/200
<input type="checkbox"/> 4932054	June 1990	Chou et al.	380/4
<input type="checkbox"/> 4937863	June 1990	Robert et al.	380/4
<input type="checkbox"/> 4953209	August 1990	Ryder, Sr. et al.	380/23
<input type="checkbox"/> 4961142	October 1990	Elliott et al.	364/408
<input type="checkbox"/> 4977594	December 1990	Shear	380/4
<input type="checkbox"/> 5010571	April 1991	Katznelson	380/4
<input type="checkbox"/> 5014234	May 1991	Edwards, Jr.	364/900
<input type="checkbox"/> 5023907	June 1991	Johnson et al.	380/4
<input type="checkbox"/> 5047928	September 1991	Wiedemer	364/406
<input type="checkbox"/> 5050213	September 1991	Shear	380/25
<input type="checkbox"/> 5058164	October 1991	Elmer et al.	380/50
<input type="checkbox"/> 5103476	April 1992	Waite et al.	380/4
<input type="checkbox"/> 5113519	May 1992	Johnson et al.	395/600
<input type="checkbox"/> 5138712	August 1992	Corbin	395/700
<input type="checkbox"/> 5146499	September 1992	Geffrotin	380/23
<input type="checkbox"/> 5159182	October 1992	Eisele	235/492
<input type="checkbox"/> 5191193	March 1993	Le Roux	235/379
<input type="checkbox"/> 5204897	April 1993	Wyman	380/4
<input type="checkbox"/> 5247575	September 1993	Sprague et al.	380/9
<input type="checkbox"/> 5255106	October 1993	Castro	380/18
<input type="checkbox"/> 5260999	November 1993	Wyman	380/4
<input type="checkbox"/> 5291596	March 1994	Mita	395/608
<input type="checkbox"/> 5339091	August 1994	Yamazaki et al.	345/104

## FOREIGN PATENT DOCUMENTS

FOREIGN-PAT-NO	PUBN-DATE	COUNTRY	US-CL
0332707	September 1989	EPX	
2236604	April 1991	GBX	
WO9220022	November 1992	WOX	
9301550	January 1993	WOX	

## OTHER PUBLICATIONS

Press Release From Electronic Publishing Resources, Inc. (EPR) entitled  
 "National Semiconductor and EPR Partner for Information Metering/Data Security

Cards", dated Mar. 4, 1994.

Weber, R., "Digital Rights Management Technology", Oct. 1995.

European Search Report for Corresponding European Application 95308417.5.

U. Flasche et al., Decentralized Processing of Documents, Comput. & Graphics, vol. 10, No. 2, 1986, pp. 119-131.

R. Mori et al., Superdistribution: The Concept and the Architecture, The Transactions of the IEICE, vol. E 73, No. 7, 1990, Tokyo, JP, pp. 1133-1146.

Weber, R., "Metering Technologies For Digital Intellectual Property," A Report to the International Federation of Reproduction Rights Organizations, Oct. 1994, pp. 1-29.

Clark, P.C. and Hoffman, L.J., "Bits: A Smartcard Protected Operating System," Communications of the ACM, Nov. 1994, vol. 37, No. 11, pp. 66-70, and 94.

Ross, P.E., "Data guard", Forbes, Jun. 6, 1994, p. 101.

Saigh, W.K., "Knowledge is Sacred," Video Pocket/Page Reader Systems, Ltd., 1992.

Kahn, R.E., "Deposit, Registration And Recordation In An Electronic Copyright Management System," Corporation for National Research Initiatives, Virginia, Aug. 1992, pp. 1-19.

Hilts, P., Mutter, J., and Taylor, S., "Books While U Wait," Publishers Weekly, Jan. 3, 1994, pp. 48-50.

Strattner, A., "Cash register on a chip" may revolutionize software pricing and distribution; Wave Systems Corp., Computer Shopper. Copyright, Apr. 1994, vol. 14; No. 4; p. 62; ISSN 0886-0556.

O'Conner, M.A., "New distribution option for electronic publishers; iOpener data encryption and metering system for CD-ROM use; Column," CD-ROM Professional, Copyright, Mar. 1994, vol. 7; No. 2; p. 134; ISSN: 1049-0833.

Willett, S., "Metered PCs: Is your system watching you?"; Wave Systems beta tests new technology, InfoWorld, Copyright, May 2, 1994, p. 84.

Linn, R.J., "Copyright and Information Services in the Context of the National Research and Education Network.sup.1," IMA Intellectual Property Project Proceedings, Jan. 1994, vol. 1, Issue 1, pp. 9-20.

erritt, Jr., H.H., "Permissions Headers and Contract Law," IMA Intellectual Property Project Proceedings, Jan. 1994, vol. 1, Issue 1, pp. 27-48.

Upthegrove, L., and Roberts, R., "Intellectual Property Header Descriptors: A Dynamic Approach," IMA Intellectual Property Project Proceedings, Jan. 1994, vol. 1, Issue 1, pp. 63-66.

Sirbu, M.A., "Internet Billing Service Design and Prototype Implementation," IMA Intellectual Property Project Proceedings, Jan. 1994, vol. 1, Issue 1, pp. 67-80.

Simmel, S.S., and Godard, I., "Metering and Licensing of Resources: Kala's General Purpose Approach," IMA Intellectual Property Project Proceedings, Jan. 1994, vol. 1, Issue 1, pp. 81-110.

Kahn, R.E., "Deposit, Registration and Recordation in an Electronic Copyright Management System," IMA Intellectual Property Project Proceedings, Jan. 1994, vol. 1, Issue 1, pp. 111-120.

Tygar, J.D., and Bennet, Y., "Dyad: A System for Using Physically Secure Coprocessors," IMA Intellectual Property Project Proceedings, Jan. 1994, vol. 1, Issue 1, pp. 121-152.

Griswold, G.N., "A Method for Protecting Copyright on Networks," IMA Intellectual Property Project Proceedings, Jan. 1994, vol. 1, Issue 1, pp. 169-178.

Nelson, T.H., "A Publishing and Royalty Model for Networked Documents," IMA Intellectual Property Project Proceedings, Jan. 1994, vol. 1, Issue 1, pp. 257-259.

ART-UNIT: 232

PRIMARY-EXAMINER: Pan; Daniel H.

ATTY-AGENT-FIRM: Domingo; Richard B.

#### ABSTRACT:

A system for controlling use and distribution of digital works. The present invention allows the owner of a digital work to attach usage rights to their work. The usage rights define how the individual digital work may be used and distributed. Instances of usage rights are defined using a flexible and extensible usage rights grammar. Conceptually, a right in the usage rights grammar is a label associated with a predetermined behavior and conditions to exercising the right. The behavior of a usage right is embodied in a predetermined set of usage transactions steps. The usage transaction steps

further check all conditions which must be satisfied before the right may be exercised. These usage transaction steps define a protocol for requesting the exercise of a right and the carrying out of a right.

28 Claims, 20 Drawing figures

**WEST**

## End of Result Set



Generate Collection

L7: Entry 4 of 4

File: DWPI

Oct 5, 2000

DERWENT-ACC-NO: 2000-647267

DERWENT-WEEK: 200121

COPYRIGHT 2001 DERWENT INFORMATION LTD

TITLE: Enforcement architecture for digital rights management, determines whether right to render digital content in manner sought exists based on digital license stored in computing device

INVENTOR: ABBURI, R; BELL, J R C ; BLINN, A N ; ENGLAND, P ; JAKUBOWSKI, M H ; JONES, T C ; MANFERDELLI, J L ; PEINADO, M ; VENKATESAN, R ; YU, H Y V

## PATENT-ASSIGNEE:

ASSIGNEE

CODE

MICROSOFT CORP

MICRN

PRIORITY-DATA: 1999US-0290363 (April 12, 1999), 1999US-0126614 (March 27, 1999)

## PATENT-FAMILY:

PUB-NO	PUB-DATE	LANGUAGE	PAGES	MAIN-IPC
WO 200059150 A2	October 5, 2000	E	090	H04L009/00
AU 200035039 A	October 16, 2000		000	H04L009/00

DESIGNATED-STATES: AE AL AM AT AU AZ BA BB BG BR BY CA CH CN CR CU CZ DE DK DM EE ES FI GB GD GE GH GM HR HU ID IL IN IS JP KE KG KP KR KZ LC LK LR LS LT LU LV MA MD MG MK MN MW MX NO NZ PL PT RO RU SD SE SG SI SK SL TJ TM TR TT TZ UA UG UZ VN YU ZA ZW AT BE CH CY DE DK EA ES FI FR GB GH GM GR IE IT KE LS LU MC MW NL OA PT SD SE SL SZ TZ UG ZW

## APPLICATION-DATA:

PUB-NO	APPL-DATE	APPL-NO	DESCRIPTOR
WO 200059150A2	February 25, 2000	2000WO-US04947	
AU 200035039A	February 25, 2000	2000AU-0035039	
AU 200035039A		WO 200059150	Based on

INT-CL (IPC): H04L 9/00

RELATED-ACC-NO: 2000-611744;2000-647268 ;2001-090815 ;2001-191170 ;2001-210824 ;2001-210825

ABSTRACTED-PUB-NO: WO 200059150A

## BASIC-ABSTRACT:

NOVELTY - A computing device (14) receives distributed digital content from a content server (22) and stores digital license corresponding to the digital content (12). A digital rights management (DRM) system on the computing device is invoked by a rendering application and determines whether a right to render digital content in the manner sought exists based on digital license stored in the computing device.

DETAILED DESCRIPTION - The digital content (12) in encrypted form is distributed by content server and a license server (24) issues digital license corresponding to the digital content. The content and license servers are communicatively coupled to internet. The digital license includes a decryption key for decrypting the encrypted digital content and a description of rights conferred by the license. An INDEPENDENT CLAIM is also included for digital rights management implementing method.

USE - For allowing access to digital contents such as digital audio, video, text and digital multimedia and enforcing rights in protected digital content on a medium such as internet, optical disk. For handheld devices, multiprocessor systems, microprocessor based or programmable consumer electronics, network PCs, mini computers, main frame computers.

ADVANTAGE - Prevents user of the computing device from making a copy of digital content, except otherwise allowed by content owner. Enables user to obtain license from a license server without any action necessary on the part of the user.

DESCRIPTION OF DRAWING(S) - The figure shows block diagram of enforcement architecture.

Digital content 12

Computing device 14

Servers 22,24

CHOSEN-DRAWING: Dwg.1/12

TITLE-TERMS: ARCHITECTURE DIGITAL MANAGEMENT DETERMINE RIGHT RENDER DIGITAL CONTENT MANNER EXIST BASED DIGITAL LICENCE STORAGE COMPUTATION DEVICE

DERWENT-CLASS: W01

EPI-CODES: W01-A05; W01-A05A;

SECONDARY-ACC-NO:

Non-CPI Secondary Accession Numbers: N2000-479688

**WEST**

Generate Collection

L7: Entry 2 of 4

File: DWPI

Oct 16, 2000

DERWENT-ACC-NO: 2001-210825

DERWENT-WEEK: 200121

COPYRIGHT 2001 DERWENT INFORMATION LTD

TITLE: Digital rights management system for enforcing rights in digital content, has license evaluator that determines if corresponding stored license enables requesting user to render requested digital content

INVENTOR: ABBURI, R; BELL, J R C ; PEINADO, M

PATENT-ASSIGNEE:

ASSIGNEE

CODE

MICROSOFT CORP

MICRN

PRIORITY-DATA: 2000US-0482932 (January 13, 2000), 1999US-0126614 (March 27, 1999), 1999US-0290363 (April 12, 1999)

PATENT-FAMILY:

PUB-NO	PUB-DATE	LANGUAGE	PAGES	MAIN-IPC
AU 200037101 A	October 16, 2000		000	G06F001/00
WO 200058811 A2	October 5, 2000	E	080	G06F001/00

DESIGNATED-STATES: AE AL AM AT AU AZ BA BB BG BR BY CA CH CN CR CU CZ DE DK DM EE ES FI GB GD GE GH GM HR HU ID IL IN IS JP KE KG KP KR KZ LC LK LR LS LT LU LV MA MD MG MK MN MW MX NO NZ PL PT RO RU SD SE SG SI SK SL TJ TM TR TT TZ UA UG UZ VN YU ZA ZW AT BE CH CY DE DK EA ES FI FR GB GH GM GR IE IT KE LS LU MC MW NL OA PT SD SE SL SZ TZ UG ZW

APPLICATION-DATA:

PUB-NO	APPL-DATE	APPL-NO	DESCRIPTOR
AU 200037101A	February 25, 2000	2000AU-0037101	
AU 200037101A		WO 200058811	Based on
WO 200058811A2	February 25, 2000	2000WO-US05091	

INT-CL (IPC): G06F 1/00

RELATED-ACC-NO: 2000-611744;2000-647267 ;2000-647268 ;2001-090815 ;2001-191170 ;2001-210824

ABSTRACTED-PUB-NO: WO 200058811A

BASIC-ABSTRACT:

NOVELTY - The DRM system has a license store (38) that stores digital licenses on a computer (14). A license evaluator (38) determines if a corresponding license in the license store enables the requesting user to render requested digital content in the manner sought based on reviewed license rules. A state store (40) holds the state data corresponding to the each stored license.

DETAILED DESCRIPTION - The license evaluator also determines if the stored licenses correspond to a requested digital content and if the corresponding

licenses are valid, and reviews license rules in each valid license. The state data are created and updated by the license evaluator as necessary. INDEPENDENT CLAIMS are also included for the following:

- (a) the computer used in the DRM system;
- (b) the computer-readable medium storing computer-executable instructions for operating the DRM system;
- (c) and the acquisition and execution of the valid license.

USE - For enforcing rights in digital content e.g. digital audio, digital video, digital text, digital data, digital multimedia.

ADVANTAGE - Allows access to encrypted digital content in accordance to specified parameters by license rights acquired by a user of the digital content. Allows owner of digital content to specify license rules that must be satisfied before digital content is allowed to be rendered on user's computer. Can be used in other computer system configurations e.g. handheld devices, multiprocessor systems, microprocessor-based or programmable consumer electronics, network PCs, minicomputers, mainframe computers. Can also be used in distributed computer environments where tasks are performed by remote processing devices linked through a communications network. Uses programming that is straight-forward for relevant programming public.

DESCRIPTION OF DRAWING(S) - The figure shows the block diagram of the user's computer in the DRM system.

Computer 14

License evaluator 38

License store 38

State store 40

CHOSEN-DRAWING: Dwg.4/12

TITLE-TERMS: DIGITAL MANAGEMENT SYSTEM ENFORCE DIGITAL CONTENT LICENCE EVALUATE  
DETERMINE CORRESPOND STORAGE LICENCE ENABLE REQUEST USER RENDER REQUEST DIGITAL  
CONTENT

DERWENT-CLASS: T01 T03

EPI-CODES: T01-J12C; T01-S03; T03-P07;

SECONDARY-ACC-NO:

Non-CPI Secondary Accession Numbers: N2001-150658

**WEST**☐ **Generate Collection**

L3: Entry 2 of 4

File: USPT

May 29, 2001

US-PAT-NO: 6240185

DOCUMENT-IDENTIFIER: US 6240185 B1

TITLE: Steganographic techniques for securely delivering electronic digital rights management control information over insecure communication channels

DATE-ISSUED: May 29, 2001

## INVENTOR-INFORMATION:

NAME	CITY	STATE	ZIP CODE	COUNTRY
Van Wie; David M.	Eugene	OR		
Weber; Robert P.	Menlo Park	CA		

## ASSIGNEE-INFORMATION:

NAME	CITY	STATE	ZIP CODE	COUNTRY	TYPE	CODE
Intertrust Technologies Corporation	Santa Clara	CA			02	

APPL-NO: 9/ 247328

DATE FILED: February 10, 1999

## PARENT-CASE:

CROSS REFERENCE TO RELATED APPLICATION This application is a continuation of Ser. No. 08/689,606, filed Aug. 12, 1996, now U.S. Pat. No. 5,943,422, issued Aug. 24, 1999, which is herein incorporated by reference; and This application is related to commonly assigned copending application Ser. No. 08/388,107 of Ginter et al., filed Feb. 13, 1995, entitled "SYSTEMS AND METHODS FOR SECURE TRANSACTION MANAGEMENT AND ELECTRONIC RIGHTS PROTECTION" (now abandoned). We incorporate by reference, into this application, the entire disclosure of this prior-filed Ginter et al. patent application just as if its entire written specification and drawings were expressly set forth in this application.

INT-CL: [7] H04N 7/167

US-CL-ISSUED: 380/232; 380/205, 380/210, 380/221, 380/227, 380/231, 713/189, 713/193, 713/200, 713/176, 705/51, 705/52, 705/54, 705/55, 705/59, 705/76  
US-CL-CURRENT: 380/232; 380/205, 380/210, 380/221, 380/227, 380/231, 705/51, 705/52, 705/54, 705/55, 705/59, 705/76, 713/176, 713/189, 713/193, 713/200

FIELD-OF-SEARCH: 705/26, 705/30, 705/35, 705/39-44, 705/50, 705/51, 705/55-59, 705/52-54, 705/64, 705/76, 380/3, 380/4, 380/5, 380/9, 380/23, 380/24, 380/25, 380/49, 380/50, 380/54, 380/59, 380/201, 380/202, 380/203, 380/210, 380/221, 380/223, 380/227-234, 380/239, 380/241, 380/242, 382/100, 382/232, 382/233, 713/189, 713/193, 713/194, 713/200, 713/168, 713/176

PRIOR-ART-DISCLOSED:

U.S. PATENT DOCUMENTS

**Search Selected****Search ALL**

PAT-NO

ISSUE-DATE

PATENTEE-NAME

US-CL



4112421

September 1978

Freeny

N/A

<input type="checkbox"/>	4120030	October 1978	Johnstone	N/A
<input type="checkbox"/>	4163280	July 1979	Mori et al.	N/A
<input type="checkbox"/>	4168396	September 1979	Best	N/A
<input type="checkbox"/>	4196310	April 1980	Forman et al.	N/A
<input type="checkbox"/>	4200913	April 1980	Kuhar et al.	N/A
<input type="checkbox"/>	4209787	June 1980	Freeny	N/A
<input type="checkbox"/>	4217588	August 1980	Freeny	N/A
<input type="checkbox"/>	4220991	September 1980	Hamano et al.	N/A
<input type="checkbox"/>	4232193	November 1980	Gerard	N/A
<input type="checkbox"/>	4232317	November 1980	Freeny	N/A
<input type="checkbox"/>	4236217	November 1980	Kennedy	N/A
<input type="checkbox"/>	4253157	February 1981	Kirschner et al.	N/A
<input type="checkbox"/>	4262329	April 1981	Bright et al.	N/A
<input type="checkbox"/>	4265371	May 1981	Desai et al.	N/A
<input type="checkbox"/>	4270182	May 1981	Asija	N/A
<input type="checkbox"/>	4278837	July 1981	Best	N/A
<input type="checkbox"/>	4305131	December 1981	Best	N/A
<input type="checkbox"/>	4306289	December 1981	Lumley	N/A
<input type="checkbox"/>	4309569	January 1982	Merkle	N/A
<input type="checkbox"/>	4319079	March 1982	Best	N/A
<input type="checkbox"/>	4323921	April 1982	Guillou	N/A
<input type="checkbox"/>	4328544	May 1982	Baldwin et al.	N/A
<input type="checkbox"/>	4337483	June 1982	Guillou	N/A
<input type="checkbox"/>	4361877	November 1982	Dyer et al.	N/A
<input type="checkbox"/>	4375579	March 1983	Davidson et al.	N/A
<input type="checkbox"/>	4433207	February 1984	Best	N/A
<input type="checkbox"/>	4434464	February 1984	Suzuki et al.	N/A
<input type="checkbox"/>	4442486	April 1984	Mayer	N/A
<input type="checkbox"/>	4446519	May 1984	Thomas	N/A
<input type="checkbox"/>	4454594	June 1984	Heffron et al.	N/A
<input type="checkbox"/>	4458315	July 1984	Uchenick	N/A
<input type="checkbox"/>	4462076	July 1984	Smith	N/A
<input type="checkbox"/>	4462078	July 1984	Ross	N/A
<input type="checkbox"/>	4465901	August 1984	Best	N/A
<input type="checkbox"/>	4471163	September 1984	Donald et al.	N/A
<input type="checkbox"/>	4484217	November 1984	Block et al.	N/A
<input type="checkbox"/>	4494156	January 1985	Kadison et al.	N/A
<input type="checkbox"/>	4513174	April 1985	Herman	N/A

<input type="checkbox"/>	<u>4528588</u>	July 1985	Lofberg	N/A
<input type="checkbox"/>	<u>4528643</u>	July 1985	Freeny	N/A
<input type="checkbox"/>	<u>4553252</u>	November 1985	Egendorf	N/A
<input type="checkbox"/>	<u>4558176</u>	December 1985	Arnold et al.	N/A
<input type="checkbox"/>	<u>4558413</u>	December 1985	Schmidt et al.	N/A
<input type="checkbox"/>	<u>4562306</u>	December 1985	Chou et al.	N/A
<input type="checkbox"/>	<u>4562495</u>	December 1985	Bond et al.	N/A
<input type="checkbox"/>	<u>4577289</u>	March 1986	Comerford et al.	N/A
<input type="checkbox"/>	<u>4584641</u>	April 1986	Guglielmino	N/A
<input type="checkbox"/>	<u>4588991</u>	May 1986	Atalla	N/A
<input type="checkbox"/>	<u>4589064</u>	May 1986	Chiba et al.	N/A
<input type="checkbox"/>	<u>4593353</u>	June 1986	Pickholtz	N/A
<input type="checkbox"/>	<u>4593376</u>	June 1986	Volk	N/A
<input type="checkbox"/>	<u>4595950</u>	June 1986	Lofberg	N/A
<input type="checkbox"/>	<u>4597058</u>	June 1986	Izumi et al.	N/A
<input type="checkbox"/>	<u>4634807</u>	January 1987	Chorley et al.	N/A
<input type="checkbox"/>	<u>4644493</u>	February 1987	Chandra et al.	N/A
<input type="checkbox"/>	<u>4646234</u>	February 1987	Tolman et al.	N/A
<input type="checkbox"/>	<u>4652990</u>	March 1987	Pailen et al.	N/A
<input type="checkbox"/>	<u>4658093</u>	April 1987	Hellman	N/A
<input type="checkbox"/>	<u>4670857</u>	June 1987	Rackman	N/A
<input type="checkbox"/>	<u>4672572</u>	June 1987	Alsberg	N/A
<input type="checkbox"/>	<u>4677434</u>	June 1987	Fascenda	N/A
<input type="checkbox"/>	<u>4680731</u>	July 1987	Izumi et al.	N/A
<input type="checkbox"/>	<u>4683553</u>	July 1987	Mollier	N/A
<input type="checkbox"/>	<u>4685056</u>	August 1987	Barnsdale et al.	N/A
<input type="checkbox"/>	<u>4688169</u>	August 1987	Joshi	N/A
<input type="checkbox"/>	<u>4691350</u>	September 1987	Kleijne et al.	N/A
<input type="checkbox"/>	<u>4696034</u>	September 1987	Wiedemer	N/A
<input type="checkbox"/>	<u>4701846</u>	October 1987	Ikeda et al.	N/A
<input type="checkbox"/>	<u>4712238</u>	December 1987	Gilhousen et al.	N/A
<input type="checkbox"/>	<u>4713753</u>	December 1987	Boebert et al.	N/A
<input type="checkbox"/>	<u>4740890</u>	April 1988	William	N/A
<input type="checkbox"/>	<u>4747139</u>	May 1988	Taaffe	N/A
<input type="checkbox"/>	<u>4757533</u>	July 1988	Allen et al.	N/A
<input type="checkbox"/>	<u>4757534</u>	July 1988	Matyas et al.	N/A
<input type="checkbox"/>	<u>4768087</u>	August 1988	Taub et al.	N/A
<input type="checkbox"/>	<u>4791565</u>	December 1988	Dunham et al.	N/A

<input type="checkbox"/>	<u>4796181</u>	January 1989	Wiedemer	N/A
<input type="checkbox"/>	<u>4799156</u>	January 1989	Shavit	N/A
<input type="checkbox"/>	<u>4807288</u>	February 1989	Ugon et al.	N/A
<input type="checkbox"/>	<u>4817140</u>	March 1989	Chandra et al.	N/A
<input type="checkbox"/>	<u>4823264</u>	April 1989	Deming	N/A
<input type="checkbox"/>	<u>4827508</u>	May 1989	Shear	N/A
<input type="checkbox"/>	<u>4858121</u>	August 1989	Barber et al.	N/A
<input type="checkbox"/>	<u>4864494</u>	September 1989	Kobus	N/A
<input type="checkbox"/>	<u>4868877</u>	September 1989	Fischer	N/A
<input type="checkbox"/>	<u>4903296</u>	February 1990	Chandra et al.	N/A
<input type="checkbox"/>	<u>4924378</u>	May 1990	Hershey et al.	N/A
<input type="checkbox"/>	<u>4930073</u>	May 1990	Cina	N/A
<input type="checkbox"/>	<u>4949187</u>	August 1990	Cohen	N/A
<input type="checkbox"/>	<u>4977594</u>	December 1990	Shear	N/A
<input type="checkbox"/>	<u>4999806</u>	March 1991	Chernow et al.	N/A
<input type="checkbox"/>	<u>5001752</u>	March 1991	Fischer	N/A
<input type="checkbox"/>	<u>5005122</u>	April 1991	Griffin et al.	N/A
<input type="checkbox"/>	<u>5005200</u>	April 1991	Fischer	N/A
<input type="checkbox"/>	<u>5010571</u>	April 1991	Katznelson	N/A
<input type="checkbox"/>	<u>5023907</u>	June 1991	Johnson et al.	N/A
<input type="checkbox"/>	<u>5047928</u>	September 1991	Wiedemer	N/A
<input type="checkbox"/>	<u>5048085</u>	September 1991	Abraham et al.	N/A
<input type="checkbox"/>	<u>5050213</u>	September 1991	Shear	N/A
<input type="checkbox"/>	<u>5091966</u>	February 1992	Bloomberg et al.	N/A
<input type="checkbox"/>	<u>5103392</u>	April 1992	Mori	N/A
<input type="checkbox"/>	<u>5103476</u>	April 1992	Waite et al.	N/A
<input type="checkbox"/>	<u>5111390</u>	May 1992	Ketcham	N/A
<input type="checkbox"/>	<u>5119493</u>	June 1992	Janis et al.	N/A
<input type="checkbox"/>	<u>5128525</u>	July 1992	Stearns et al.	N/A
<input type="checkbox"/>	<u>5136643</u>	August 1992	Fischer	N/A
<input type="checkbox"/>	<u>5136646</u>	August 1992	Haber et al.	N/A
<input type="checkbox"/>	<u>5136647</u>	August 1992	Haber et al.	N/A
<input type="checkbox"/>	<u>5136716</u>	August 1992	Harvey et al.	N/A
<input type="checkbox"/>	<u>5146575</u>	September 1992	Nolan	N/A
<input type="checkbox"/>	<u>5148481</u>	September 1992	Abraham et al.	N/A
<input type="checkbox"/>	<u>5155680</u>	October 1992	Wiedemer	N/A
<input type="checkbox"/>	<u>5168147</u>	December 1992	Bloomberg	N/A
<input type="checkbox"/>	<u>5185717</u>	February 1993	Mori	N/A

<input type="checkbox"/>	<u>5201046</u>	April 1993	Goldberg et al.	N/A
<input type="checkbox"/>	<u>5201047</u>	April 1993	Maki et al.	N/A
<input type="checkbox"/>	<u>5208748</u>	May 1993	Flores et al.	N/A
<input type="checkbox"/>	<u>5214702</u>	May 1993	Fischer	N/A
<input type="checkbox"/>	<u>5216603</u>	June 1993	Flores et al.	N/A
<input type="checkbox"/>	<u>5221833</u>	June 1993	Hecht	N/A
<input type="checkbox"/>	<u>5222134</u>	June 1993	Waite et al.	N/A
<input type="checkbox"/>	<u>5224160</u>	June 1993	Paulini et al.	N/A
<input type="checkbox"/>	<u>5224163</u>	June 1993	Gasser et al.	N/A
<input type="checkbox"/>	<u>5235642</u>	August 1993	Wobber et al.	N/A
<input type="checkbox"/>	<u>5245165</u>	September 1993	Zhang	N/A
<input type="checkbox"/>	<u>5247575</u>	September 1993	Sprague et al.	N/A
<input type="checkbox"/>	<u>5260999</u>	November 1993	Wyman	N/A
<input type="checkbox"/>	<u>5263158</u>	November 1993	Janis	N/A
<input type="checkbox"/>	<u>5265164</u>	November 1993	Matyas et al.	N/A
<input type="checkbox"/>	<u>5276735</u>	January 1994	Boebert et al.	N/A
<input type="checkbox"/>	<u>5280479</u>	January 1994	Mary	N/A
<input type="checkbox"/>	<u>5285494</u>	February 1994	Sprecher et al.	N/A
<input type="checkbox"/>	<u>5301231</u>	April 1994	Abraham et al.	N/A
<input type="checkbox"/>	<u>5311591</u>	May 1994	Fischer	N/A
<input type="checkbox"/>	<u>5319705</u>	June 1994	Halter et al.	N/A
<input type="checkbox"/>	<u>5319785</u>	June 1994	Halter et al.	N/A
<input type="checkbox"/>	<u>5337360</u>	August 1994	Fischer	N/A
<input type="checkbox"/>	<u>5341429</u>	August 1994	Stringer et al.	N/A
<input type="checkbox"/>	<u>5343527</u>	August 1994	Moore et al.	N/A
<input type="checkbox"/>	<u>5347579</u>	September 1994	Blandford	N/A
<input type="checkbox"/>	<u>5351293</u>	September 1994	Michener et al.	N/A
<input type="checkbox"/>	<u>5355474</u>	October 1994	Thuraisingham et al.	N/A
<input type="checkbox"/>	<u>5373561</u>	December 1994	Haber et al.	N/A
<input type="checkbox"/>	<u>5390247</u>	February 1995	Fischer	N/A
<input type="checkbox"/>	<u>5390330</u>	February 1995	Talati	N/A
<input type="checkbox"/>	<u>5392220</u>	February 1995	van den Hamer et al.	N/A
<input type="checkbox"/>	<u>5392390</u>	February 1995	Crozier	N/A
<input type="checkbox"/>	<u>5394469</u>	February 1995	Nagel et al.	N/A
<input type="checkbox"/>	<u>5410598</u>	April 1995	Shear	N/A
<input type="checkbox"/>	<u>5412717</u>	May 1995	Fischer	N/A
<input type="checkbox"/>	<u>5421006</u>	May 1995	Jablon	N/A
<input type="checkbox"/>	<u>5422953</u>	June 1995	Fischer	N/A

<input type="checkbox"/>	5428606	June 1995	Moskowitz	N/A
<input type="checkbox"/>	5438508	August 1995	Wyman	N/A
<input type="checkbox"/>	5442645	August 1995	Ugon	N/A
<input type="checkbox"/>	5444779	August 1995	Daniele	N/A
<input type="checkbox"/>	5449895	September 1995	Hecht et al.	N/A
<input type="checkbox"/>	5449896	September 1995	Hecht et al.	N/A
<input type="checkbox"/>	5450493	September 1995	Maher	N/A
<input type="checkbox"/>	5453601	September 1995	Rosen	N/A
<input type="checkbox"/>	5453605	September 1995	Hecht et al.	N/A
<input type="checkbox"/>	5455407	October 1995	Rosen	N/A
<input type="checkbox"/>	5455861	October 1995	Faucher et al.	N/A
<input type="checkbox"/>	5455953	October 1995	Russell	N/A
<input type="checkbox"/>	5457746	October 1995	Dolphin	N/A
<input type="checkbox"/>	5463565	October 1995	Cookson et al.	N/A
<input type="checkbox"/>	5473687	December 1995	Lipscomb et al.	N/A
<input type="checkbox"/>	5473692	December 1995	Davis	N/A
<input type="checkbox"/>	5479509	December 1995	Ugon	N/A
<input type="checkbox"/>	5485622	January 1996	Yamaki	N/A
<input type="checkbox"/>	5491800	February 1996	Goldsmith et al.	N/A
<input type="checkbox"/>	5497479	March 1996	Hornbuckle	N/A
<input type="checkbox"/>	5497491	March 1996	Mitchell et al.	N/A
<input type="checkbox"/>	5499298	March 1996	Narasimhalu et al.	N/A
<input type="checkbox"/>	5504757	April 1996	Cook et al.	N/A
<input type="checkbox"/>	5504818	April 1996	Okano	N/A
<input type="checkbox"/>	5504837	April 1996	Griffeth et al.	N/A
<input type="checkbox"/>	5508913	April 1996	Yamamoto et al.	N/A
<input type="checkbox"/>	5509070	April 1996	Schull	N/A
<input type="checkbox"/>	5513261	April 1996	Maher	N/A
<input type="checkbox"/>	5530235	June 1996	Stefik et al.	N/A
<input type="checkbox"/>	5530752	June 1996	Rubin	N/A
<input type="checkbox"/>	5533123	July 1996	Force et al.	N/A
<input type="checkbox"/>	5534975	July 1996	Stefik et al.	N/A
<input type="checkbox"/>	5537526	July 1996	Anderson et al.	N/A
<input type="checkbox"/>	5539735	July 1996	Moskowitz	N/A
<input type="checkbox"/>	5539828	July 1996	Davis	N/A
<input type="checkbox"/>	5550971	August 1996	Brunner et al.	N/A
<input type="checkbox"/>	5553282	September 1996	Parrish et al.	N/A
<input type="checkbox"/>	5557518	September 1996	Rosen	N/A

<input type="checkbox"/>	5563946	October 1996	Cooper et al.	N/A
<input type="checkbox"/>	5568552	October 1996	Davis	N/A
<input type="checkbox"/>	5572673	November 1996	Shurts	N/A
<input type="checkbox"/>	5592549	January 1997	Nagel et al.	N/A
<input type="checkbox"/>	5606609	February 1997	Houser et al.	N/A
<input type="checkbox"/>	5613004	March 1997	Cooperman et al.	N/A
<input type="checkbox"/>	5621797	April 1997	Rosen	N/A
<input type="checkbox"/>	5629980	May 1997	Stefik et al.	N/A
<input type="checkbox"/>	5633932	May 1997	Davis et al.	N/A
<input type="checkbox"/>	5634012	May 1997	Stefik et al.	N/A
<input type="checkbox"/>	5636292	June 1997	Rhoads	N/A
<input type="checkbox"/>	5638443	June 1997	Stefik	N/A
<input type="checkbox"/>	5638504	June 1997	Scott et al.	N/A
<input type="checkbox"/>	5640546	June 1997	Gopinath et al.	N/A
<input type="checkbox"/>	5655077	August 1997	Jones et al.	N/A
<input type="checkbox"/>	5687236	November 1997	Moskowitz et al.	N/A
<input type="checkbox"/>	5689587	November 1997	Bender et al.	N/A
<input type="checkbox"/>	5692180	November 1997	Lee	N/A
<input type="checkbox"/>	5710834	January 1998	Rhoads	N/A
<input type="checkbox"/>	5740549	April 1998	Reilly et al.	N/A
<input type="checkbox"/>	5745569	April 1998	Moskowitz et al.	380/4
<input type="checkbox"/>	5745604	April 1998	Rhoads	N/A
<input type="checkbox"/>	5748763	May 1998	Rhoads	382/232 X
<input type="checkbox"/>	5748783	May 1998	Rhoads	N/A
<input type="checkbox"/>	5748960	May 1998	Fischer	N/A
<input type="checkbox"/>	5754849	May 1998	Dyer et al.	N/A
<input type="checkbox"/>	5757914	May 1998	McManis	N/A
<input type="checkbox"/>	5758152	May 1998	LeTourneau	N/A
<input type="checkbox"/>	5765152	June 1998	Erickson	N/A
<input type="checkbox"/>	5768426	June 1998	Rhoads	N/A
<input type="checkbox"/>	5832119	November 1998	Rhoads	382/232
<input type="checkbox"/>	5896454	April 1999	Cookson et al.	380/5
<input type="checkbox"/>	5940505	August 1999	Kanamaru	705/58
<input type="checkbox"/>	6009170	December 1999	Sako et al.	380/201

## FOREIGN PATENT DOCUMENTS

FOREIGN-PAT-NO  
9 004 79

PUBN-DATE  
December 1984

COUNTRY  
BEX

US-CL

3803982A1	January 1990	DEX
0 084 441 A1	July 1983	EPX
0 135 422 A1	March 1985	EPX
0 180 460 A1	May 1986	EPX
0 370 146 A1	November 1988	EPX
0 456 386 A2	November 1991	EPX
0 469 864 A2	February 1992	EPX
0 593 305 A2	April 1994	EPX
0 651 554 A1	May 1995	EPX
0 668 695 A2	August 1995	EPX
0 695 985 A1	February 1996	EPX
0 696 798 A1	February 1996	EPX
0 714 204 A2	May 1996	EPX
0 715 244 A1	June 1996	EPX
0 715 243 A1	June 1996	EPX
0 715 245 A1	June 1996	EPX
0 715 246 A1	June 1996	EPX
0 715 247 A1	June 1996	EPX
0 725 376 A2	August 1996	EPX
0 763 936 A2	September 1996	EPX
0 749 081 A1	December 1996	EPX
0 778 513 A2	June 1997	EPX
0 795 873 A2	September 1997	EPX
0 800 312 A1	October 1997	EPX
2136175	September 1984	GBX
2294348	April 1996	GBX
2295947	June 1996	GBX
57-726	May 1982	JPX
62-241061	October 1987	JPX
1-068835	March 1989	JPX
64-68835	March 1989	JPX
2-242352	September 1990	JPX
2-247763	October 1990	JPX
2-294855	December 1990	JPX
4-369068	December 1992	JPX
5-181734	July 1993	JPX
5-257783	October 1993	JPX
5-268415	October 1993	JPX
6-175794	June 1994	JPX
6-215010	August 1994	JPX
7-056794	March 1995	JPX
7-084852	March 1995	JPX
7-141138	June 1995	JPX
7-200317	August 1995	JPX
7-200492	August 1995	JPX
7-244639	September 1995	JPX
8-137795	May 1996	JPX
8-152990	June 1996	JPX
8-185298	July 1996	JPX
WO 85/02310	May 1985	WOX
WO 85/03584	August 1985	WOX
WO 92/06438	April 1992	WOX
WO 93/01550	January 1993	WOX

WO 94/01821	January 1994	WOX
WO 94/16395	July 1994	WOX
WO 94/18620	August 1994	WOX
WO 94/22266	September 1994	WOX
WO 94/27406	November 1994	WOX
WO 96/00963	January 1996	WOX
WO 96/06503	February 1996	WOX
WO 96/03835	February 1996	WOX
WO 96/05698	February 1996	WOX
WO 96/13013	May 1996	WOX
WO 96/21192	July 1996	WOX
WO 97/03423	January 1997	WOX
WO 97/07656	March 1997	WOX
WO 97/25816	July 1997	WOX
WO 97/32251	September 1997	WOX
WO 97/48203	December 1997	WOX

## OTHER PUBLICATIONS

Michael Baum, "Worldwide Electronic Commerce: Law, Policy and Controls Conference," Nov. 11, 1993, 18 pages.

Richard L. Bisbey, II and Gerald J. Popek, Encapsulation: An Approach to Operating System Security, (USC/Information Science Institute, Marina Del Rey, CA), Oct. 1973, pp. 666-675.

Rolf Blom, Robert Forchheimer, et al., Encryption Methods in Data Networks, Ericsson Technics, No. 2, Stockholm, Sweden, 1978.

Rick E. Bruner, Document from the Internet: PowerAgent, NetBot help advertisers reach Internet shoppers, Aug. 1997, 3 pages.

Denise Caruso, Technology, Digital Commerce: 2 plans for watermarks, which can bind proof of authorship to electronic works, N.Y. Times, Aug. 7, 1995, p. D5.

A.K. Choudhury, N. F. Maxemchuck, et al., Copyright Protection for Electronic Publishing Over Computer Networks, (AT&T Bell Laboratories, Murray Hill, N. J.) Jun. 1994, 17 pages.

Tim Clark, Ad service gives cash back, Document from the Internet: (visited Aug. 4, 1997), 2 pages.

Donna Cunningham, David Arneke, et al., Document from the Internet: AT&T, VLSI Technology join to improve info highway security, ( News Release) Jan. 31, 1995, 3 pages.

Lorcan Dempsey and Stuart Weibel, The Warwick Metadata Workshop: A Framework for the Deployment of Resource Description, D-Lib Magazine, Jul. 15, 1996.

Dorothy E. Denning and Peter J. Denning, Data Security, 11 Computing Surveys No. 3, Sep. 1979, pp. 227-249.

Whitfield Diffie and Martin E. Hellman, New Directions in Cryptography, IEEE Transactions on Information Theory, vol. 22, No. 6, No. 1976, pp. 644-651.

Whitfield Diffie and Martin E. Hellman, Privacy and Authentication: An Introduction to Cryptography, Proceedings of the IEEE, vol. 67, No. 3, Mar. 1979, pp. 397-427.

Stephen R. Dusse and Burton S. Kaliski, A Cryptographic Library for the Motorola 56000, Advances in Cryptology-Proceedings of Eurocrypt 90, (I.M. Damgard, ed., Springer-Verlag) 1991, pp. 230-244.

Esther Dyson, Intellectual Value, WIRED Magazine, Jul. 1995, pp. 136-141 and 182-183.

James Gleick, Dead as a Dollar, The New York Times Magazine, Jun. 16, 1996, Sect. 6, pp. 26-30, 35, 42, 50, 54.

Fred Greguras, Document from Internet: Softic Symposium '95, Copyright Clearances and Moral Rights, Dec. 11, 1995, 3 pages.

Louis C. Guillou, Smart Cards and Conditional Access, Advances in Cryptography--Proceedings of EuroCrypt 84 (T. Beth et al, Ed., Springer-Verlag, 1985) pp. 480-490.

Harry H. Harman, Modern Factor Analysis, Third Edition Revised, University of Chicago Press, Chicago and London, 1976.

Amir Herzberg and Shlomit S. Pinter, Public Protection of Software, ACM Transactions on Computer Systems, vol. 5, No. 4, Nov. 1987, pp. 371-393.

Jud Hofmann, Interfacing the NII to User Homes, (Consumer Electronic Bus.

Committee) NIST, Jul. 1994, 12 slides.

Jud Hofmann, Interfacing the NII to User Homes, Electronic Industries Association, (Consumer Electronic Bus Committee) (undated), 14 slides.

Stannie Holt, Document from the Internet: Start-up promises user confidentiality in Web marketing service, InfoWorld Electric News (updated Aug. 13, 1997).

Jay J. Jiang and David W. Conrath, A Concept-based Approach to Retrieval from an Electronic Industrial Directory, International Journal of Electronic Commerce, vol. 1, No. 1 (Fall 1996) pp. 51-72.

Debra Jones, Document from the Internet: Top Tech Stories, PowerAgent Introduces First Internet `Informediary` to Empower and Protect Consumers, (updated Aug. 13, 1997) 3 pages.

Kevin Kelly, E-Money, Whole Earth Review, Summer 1993, pp. 40-59.

Stephen Thomas Kent, Protecting Externally Supplied Software in Small Computers, (MIT/LCS/TR-255) Sep. 1980 254 pages.

David M. Kristol, Steven H. Low and Nicholas F. Maxemchuk, Anonymous Internet Mercantile Protocol, (AT&T Bell Laboratories, Murray Hill, NJ) Draft: Mar. 17, 1994.

Carl Lagoze, The Warwick Framework, A Container Architecture for Diverse Sets of Metadata, D-Lib Magazine, Jul./Aug. 1996.

Mike Lanza, e-mail, George Gilder's Fifth Article--Digital Darkhorse--Newspapers, Feb. 21, 1994.

Steven Levy, E-Money, That's What I want, WIRED, Dec. 1994, 10 pages.

Steven H. Low and Nicholas F. Maxemchuk, Anonymous Credit Cards, AT&T Bell Laboratories, Proceedings of the 2.sup.nd ACM Conference on Computer and Communication Security, Fairfax, VA, Nov. 2-4, 1994, 10 pages.

Steven H. Low, Nicholas F. Maxemchuk, and Sanjoy Paul, Anonymous Credit Cards and its Collusion Analysis (AT&T Bell Laboratories, Murray Hill, N.J.) Oct. 10, 1994, 18 pages.

S. H. Low, N.F. Maxemchuk, et al., Document Marking and Identification using both Line and word Shifting (AT&T Bell Laboratories, Murray Hill, N.J.) Jul. 29, 1994, 22 pages.

N.F. Maxemchuk, Electronic Document Distribution, (AT&T Bell Laboratories, Murray Hill, N.J.) (undated).

Nicholas Negroponte, Some Thoughts on Likely and Expected Communications Scenarios: A Rebuttal, Telecommunications, Jan. 1993, pp. 41-42.

Nicholas Negroponte, Electronic Word of Mouth, WIRED, Oct. 1996, p. 218.

Peter G. Neumann, Robert S. Boyer, et al., A Provably Secure Operating System: The System, Its Applications, and Proofs, Computer Science Laboratory Report CSL-116, Second Edition, SRI International, Jun. 1980.

Joseph N. Pelton (Dr.), Why Nicholas Negroponte is Wrong About the Future of Telecommunication, Telecommunications, Jan. 1993, pp. 35-40.

Gordon Rankine (Dr.), Thomas--A Complete Single-Chip RSA Device, Advances in Cryptography, Proceedings of CRYPTO 86, (A.M. Odiyzko Ed., Springer-Verlag) 1987, pp. 480-487.

Arthur K. Reilly, Input to the `International Telecommunications Hearings,` Panel 1: Component Technologies of the NII/GII, Standards Committee T1-Telecommunications (undated).

Paul Resnick and Hal R. Varion, Recommender Systems, Communications of the ACM, vol. 40, No. 3, Mar. 1997 pp. 56-89.

Lance Rose, Cyberspace and the Legal Matrix: Laws or Confusion?, 1991.

Steve Rosenthal, Interactive Network: Viewers Get Involved, New Media, Dec. 1992, pp. 30-31.

Steve Rosenthal, Interactive TV: The Gold Rush is on, New Media, Dec. 1992, pp. 27-29.

Steve Rosenthal, Mega Channels, New Media, Sep. 1993, pp. 36-46.

Edward Rothstein, Technology, Connections, Making the Internet come to you through `push` technology, N.Y. Times, Jan. 20, 1997, p. D5.

Ken Rutkowski, Document from Internet: PowerAgent Introduces First Internet `Informediary` to Empower and Protect Consumers, Tech Talk News Story, Aug. 4, 1997, 1 page.

Ira Sager (Edited by), Bits & Bytes, Business Week, Sep. 23, 1996, p. 142E.

Schlosstein, Steven, America: The G7's Comeback Kid, International Economy, Jun./Jul. 1993, 5 pages.

Ingrid Scaum Mueller-Bichl and Ernst Piller, A Method of Software Protection Based on the Use of Smart Cards and Cryptographic Techniques, (undated), 9 pages.

Jurgen Schurmann, Pattern Classification, A Unified View of Statistical and Neural Approaches, John Wiley & Sons, Inc., 1996.

Victor Shear, Solutions for CD-ROM Pricing and Data Security Problems, CD ROM Yearbook 1988-1989 (Microsoft Press 1988 or 1989) pp. 530-533.

Sean Smith and J.D. Tygar, Signed Vector Timestamps: A Secure Protocol for Partial Order Time, CMU-93-116, School of Computer Science Carnegie Mellon University, Pittsburgh, Pennsylvania, Oct. 1991; version of Feb. 1993, 15 pages.

Mark Stefik, Letting Loose the Light: Igniting Commerce in Electronic Publication, (Xerox PARC, Palo Alto, CA) 1994-1995, 35 pages.

Bruce Sterling, Literary freeware: Not for Commercial Use, remarks at Computers, Freedom and Private Conference IV, Chicago, IL, Mar. 26, 1994.

Bruno Struif, The Use of Chipcards for Electronic Signatures and Encryption, Proceedings for the 1989 Conference on VSLI and Computer Peripherals, IEEE Computer Society Press, 1989, pp. (4)155-(4)158.

J.D. Tygar and Bennet Yee, Cryptography: It's Not Just For Electronic Mail Anymore, CMU-CS-93-107, School of Computer Science Carnegie Mellon University, Pittsburgh, PA, Mar. 1, 1993, 21 pages.

J.D. Tygar and Bennet Yee, Dyad: A System for Using Physically Secure Coprocessors, School of Computer Science, Carnegie Mellon University, Pittsburgh, PA, May 1991, 36 pages.

T. Valovic, The Role of Computer Networking in the Emerging Virtual Marketplace, Telecommunications, (undated), pp. 40-44.

Joan Voight, Beyond the Banner, Wired, Dec. 1996, pp. 196, 200, 204.

Steven Vonder Haar, Document from the Internet: PowerAgent Launches Commercial Service, Interactive Week, Aug. 4, 1997, 1 page.

Robert Weber, Document from the Internet: Digital Rights Management Technologies, Oct. 1995, 21 pages.

Robert Weber, Digital Rights Management Technologies, A Report to the International Federation of Reproduction Rights Organisations, Northeast Consulting Resources, Inc., Oct. 1995, 49 pages.

Adele Weder, Life on the Infohighway, Insite, (undated), pp. 23-25.

Steve H. Weingart, Physical Security for the ABYSS System, (IBM Thomas J. Watson Research Center, Yorktown Heights, NY), 1987, pp. 52-58.

Daniel J Weitzner, A Statement on EFF's Open Platform Campaign as of Nov., 1993, 3 pages.

Steve R. White, ABYSS: A Trusted Architecture for Software Protection, (IBM Thomas J. Watson Research Center, Yorktown Heights, NY), 1987, pp. 38-50.

Bennet Yee, Using Secure Coprocessors, CMU-CS-94-149, School of Computer Science, Carnegie Mellon University, Pittsburgh, PA, 1994, 94 pages.

Frank Yellin, Document from the Internet: Low Level Security in Java, Sun Microsystems, 1996, 8 pages.

ART-UNIT: 362

PRIMARY-EXAMINER: Gregory; Bernarr E.

ATTY-AGENT-FIRM: Finnegan, Henderson, Farabow, Garrett & Dunner, L.L.P.

ABSTRACT:

Electronic steganographic techniques can be used to encode a rights management control signal onto an information signal carried over an insecure communications channel. Steganographic techniques ensure that the digital control information is substantially invisibly and substantially indelibly carried by the information signal. These techniques can provide end-to-end rights management protection of an information signal irrespective of transformations between analog and digital. An electronic appliance can recover the control information and use it for electronic rights management to provide compatibility with a Virtual Distribution Environment. In one example, the system encodes low data rate pointers within high bandwidth time periods of the content signal to improve overall control information read/seek times.

32 Claims, 33 Drawing figures

Exemplary Claim Number: 25

Number of Drawing Sheets: 31

BRIEF SUMMARY:

## FIELD OF THE INVENTION

The present inventions relate generally to computer security, and more particularly to steganographic techniques for hiding or encoding electronic control information within an information signal carried by an insecure communications channel. Still more particularly, the present inventions relate to systems, methods and techniques that substantially invisibly and/or indelibly convey, over analog or other insecure communications channels, digital rights management control information for use within a virtual distribution environment electronic rights management system.

## BACKGROUND AND SUMMARY OF THE INVENTION

The world is becoming digital. Digital signals are everywhere--in our computers, television sets, VCRs, home stereos, and CD players. Digital processing--which operates on information "bits" (numerical "on" or "off" values)--provides a degree of precision and protection from noise that cannot be matched by the older, "analog" formats we have used since the beginning of the electronic age.

Despite the clear advantage of digital communications, the older "analog" domain remains significant. Many of our most important information delivery mechanisms continue to be based on analog--not digital--signaling. In fact, most of our electronic entertainment, news, sports and music program material comes to us in the form of analog signals. For example:

Television remains largely analog. Although the distribution of television programming to local cable systems is increasingly digital and most modern television sets include digital signal processing circuits, the local cable television "head end" continues to send television signals to the subscriber's set top box and television in analog--not digital--form. It will cost a great deal to convert local cable distribution from analog to digital. In the United States, for example, the widespread conversion from analog to digital television is projected to take no less than 15 years and perhaps even longer.

In radio broadcasting, too, analog communication continues to reign supreme. Thousands of radio stations broadcast music, news and other programs every day in analog form. Except for a few experimental digital systems, practically all radio broadcasting is carried over analog communications channels.

The movies and videos we rent at the local video tape rental store are analog.

Commercially available music tape cassettes are recorded in analog formats.

Moreover, the "real world" is analog. Everything digital must ultimately be turned into something analog if we are to experience it; and conversely, everything analog must be turned into something digital if the power of modern digital technology will be used to handle it. Modern digital technology also allows people to get better quality for less money.

Despite the pervasiveness of analog signals, existing methods for managing rights and protecting copyright in the analog realm are primitive or non-existent. For example:

Quality degradation inherent in multigenerational analog copying has not prevented a multi-billion dollar pirating industry from flourishing.

Some methods for video tape copy and pay per view protection attempt to prevent any copying at all of commercially released content, or allow only one generation of copying. These methods can generally be easily circumvented.

Not all existing devices respond appropriately to copy protection signals.

Existing schemes are limited for example to "copy/no copy" controls.

Copy protection for sound recordings has not been commercially implemented.

A related problem relates to the conversion of information between the analog and digital domains. Even if information is effectively protected and

controlled initially using strong digital rights management techniques, an analog copy of the same information may no longer be securely protected.

For example, it is generally possible for someone to make an analog recording of program material initially delivered in digital form. Some analog recordings based on digital originals are of quite good quality. For example, a Digital Versatile Disk ("DVD") player may convert a movie from digital to analog format and provide the analog signal to a high quality analog home VCR. The home VCR records the analog signal. A consumer now has a high quality analog copy of the original digital property. A person could re-record the analog signal on a DVD-R (a Digital Versatile Disk appliance and media supporting both read and write operations). This recording will in many circumstances have substantial quality--and would no longer be subject to "pay per view" or other digital rights management controls associated with the digital form of the same content.

Since analog formats will be with us for a long time to come, rightsholders such as film studios, video rental and distribution companies, music studios and distributors, and other value chain participants would very much like to have significantly better rights management capabilities for analog film, video, sound recordings and other content. Solving this problem generally requires a way to securely associate rights management information with the content being protected.

People have for many years been using various techniques allowing digital information to, in effect, ride "piggyback" on analog information signals. For example, since the 1960s, it has been common to digitally encode text information such as subtitles into otherwise unused portions of analog television signals (e.g., within the so-called "Vertical Blanking Interval").

Unfortunately, sending digital information using such known digital encoding techniques is problematic because the digital information is not persistent. It is relatively easy to strip out or eliminate digital information encoded using prior techniques commonly employed for superimposing digital signals onto an analog information signal. Analog communications channels may commonly be subjected to various signal processing that may (intentionally or unintentionally) strip out digital information added to the analog signal--defeating any downstream system, process or technique that depends on the presence and readability of the digital information. For example, the television vertical blanking signal--along with any signal components disposed within the vertical blanking interval--is typically routinely eliminated whenever a video signal is processed by a computer.

Attempting to use insecure techniques for providing rights management is at best ineffective, and can be worse than no rights management at all. Unscrupulous people can strip out insecure control information altogether so that the corresponding information signal is subject to no controls at all--for example, defeating copy protection mechanisms and allowing users to avoid paying for rights usage. More nefariously, an unscrupulous person could alter an insecure system by substituting false control information in place of the proper information. Such substitutions could, for example, divert payments to someone other than legitimate rights holders--facilitating electronic fraud and theft.

Prior, insecure techniques fail to solve the overall problem of how to provide and securely manage advanced automatic electronic rights management for analog and other information signals conveyed over an insecure communications channel. The lack of strong rights management for analog signals creates a huge gap in any comprehensive electronic rights management strategy, and makes it possible for consumers and others to circumvent--to at least some extent--even the strongest digital rights management technologies. Consequently, there is a real need to seamlessly integrate analog delivery models with modern electronic digital rights management techniques.

The present inventions solve these and other problems by providing "end to end" secure rights management protection allowing content providers and rights holders to be sure their content will be adequately protected--irrespective of the types of devices, signaling formats and nature of signal processing within the content distribution chain. This "end to end" protection also allows

authorized analog appliances to be easily, seamlessly and cost-effectively integrated into a modern digital rights management architecture.

The present inventions may provide a Virtual Distribution Environment ("VDE") in which electronic rights management control information may be delivered over insecure (e.g., analog) communications channels. This Virtual Distribution Environment is highly flexible and convenient, accommodating existing and new business models while also providing an unprecedented degree of flexibility in facilitating ad hoc creation of new arrangements and relationships between electronic commerce and value chain participants--regardless of whether content is distributed in digital and/or analog formats.

The present inventions additionally provide the following important and advantageous features:

An indelible and invisible, secure technique for providing rights management information.

An indelible method of associating electronic commerce and/or rights management controls with analog content such as film, video, and sound recordings.

Persistent association of the commerce and/or rights management controls with content from one end of a distribution system to the other--regardless of the number and types of transformations between signaling formats (for example, analog to digital, and digital to analog).

The ability to specify "no copy/one copy/many copies" rights management rules, and also more complex rights and transaction pricing models (such as, for example, "pay per view" and others).

The ability to fully and seamlessly integrate with comprehensive, general electronic rights management solutions (such as those disclosed in the Ginter et al. patent specification referenced above).

Secure control information delivery in conjunction with authorized analog and other non-digital and/or non-secure information signal delivery mechanisms.

The ability to provide more complex and/or more flexible commerce and/or rights management rules as content moves from the analog to the digital realm and back.

The flexible ability to communicate commerce and/or rights management rules implementing new, updated, or additional business models to authorized analog and/or digital devices.

Briefly, the present inventions use "steganography" to substantially indelibly and substantially invisibly encode rights management and/or electronic commerce rules and controls within an information signal such as, for example, an analog signal or a digitized (for example, sampled) version of an analog signal.

The Greek term "steganography" refers to various "hidden writing" secret communication techniques that allow important messages to be securely carried over insecure communications channels. Here are some examples of steganography:

In ancient Persia an important message was once tattooed on a trusted messenger's shaved scalp. The messenger then allowed his hair to grow back--completely hiding the message. Once the messenger made his way to his destination, he shaved his hair off again--exposing the secret message so the recipient could read it on the messenger's shaved scalp. See Kahn, David, *The Codebreakers* page 81 et seq. and page 513 et seq. (Macmillan 1967). This unusual technique for hiding a message is one illustration of "steganography."

Another "steganographic" technique encodes a secret message within another, routine message. For example, the message "Hey Elmer, Lisa Parked My Edsel" encodes the secret message "HELP ME"--the first letter of each word of the message forming the letters of the secret message ("Hey Elmer, Lisa Parked My Edsel"). Variations on this technique can provide additional security, but the basic concept is the same--finding a way to hide a secret message within

information that can or will be sent over an insecure channel.

Invisible ink is another commonly used "steganography" technique. The secret message is written using a special disappearing or invisible ink. The message can be written on a blank piece of paper, or more commonly, on the back or front of the piece of paper carrying a routine-looking or legitimate letter or other written communication. The recipient performs a special process on the received document (e.g., exposing it to a chemical or other process that makes the invisible ink visible) so that he or she can read the message. Anyone intercepting the paper will be unable to detect the secret message--or even know that it is there--unless the interceptor knows to look for the invisible message and also knows how to treat the paper to make the invisible ink visible.

The present inventions use steganography to ensure that encoded control information is both substantially invisible and substantially indelible as it passes over an insecure communications channel. At the receiving end, a secure, trusted component (such as a protected processing environment described in Ginter et al.) recovers the steganographically-encoded control information, and uses the recovered information to perform electronic rights management (for example, on analog or other information signals carried over the same channel).

One specific aspect provided by the present inventions involve steganographically encoding digital rights management control information onto an information signal such as, for example, an analog or digitized television, video or radio signal. The steganographic encoding process substantially inextricably intertwines the digital control information with images, sounds and/or other content the information signal carries--but preferably without noticeably degrading or otherwise affecting those images, sounds and/or other content. It may be difficult to detect (even with educated signal processing techniques) that the analog signal has been steganographically encoded with a rights management control signal, and it may be difficult to eliminate the steganographically encoded control signal without destroying or degrading the other information or content the signal carries.

The present inventions also provide a secure, trusted protected processing environment to recover the steganographically-encoded control signal from the information signal, and to enforce rights management processes based on the recovered steganographically encoded control signal. This allows the information signal delivery mechanism to be fully integrated (and made compatible) with a digital virtual distribution environment and/or other electronic rights management system.

In accordance with yet another aspect provided by this invention, steganographically encoded, digital rights management control information may be used in conjunction with a scrambled and/or encrypted information signal. The scrambling and/or encryption can be used to enforce the rights management provided in accordance with the steganographically encoded rights management control information. For example, the control signal can be steganographically decoded and used to control, at least in part, under what circumstances and/or how the information signal is to be descrambled and/or decrypted.

In accordance with yet another feature provided by the invention, digital certificates can be used to securely enforce steganographically encoded rights management control information.

In accordance with still another feature provided by the invention, steganography is used to encode an information signal with rights management control information in the form of one or more protected organizational structures having association with electronic controls. The electronic controls may, for example, define permitted and/or required operation(s) on content, and consequences of performing and/or failing to perform such operations. The organizational structure(s) may identify, implicitly or explicitly, the content the electronic controls apply to. The organizational structure(s) may also define the extent of the content, and semantics of the content.

The type, amount and characteristics of the steganographically encoded rights management control information are flexible and programmable--providing a rich,

diverse mechanism for accommodating a wide variety of rights management schemes. The control information can be used to securely enforce straightforward secure rights management consequences such as "copy/no copy/one copy" type controls--but are by no means limited to such models. To the contrary, the present invention can be used to enable and enforce much richer, more complex rights management models--including for example those involving usage auditing, automatic electronic payment, and the use of additional electronic network connections. Moreover, the rights management control arrangements provided by the present invention are infinitely extensible and scalable--fully accommodating future models as they are commercially deployed while preserving full compatibility with different (and possibly more limited) rights management models deployed during earlier stages.

The organizational structure(s) may be steganographically encoded in such a way that they are protected for purposes of secrecy and/or integrity. The employed steganographic techniques may provide some degree of secrecy protection--or other security techniques (e.g., digital encryption, digital seals, etc.) may be used to provide a desired or requisite degree of security and/or integrity protection for the steganographically encoded information.

In one example, the organizational structure(s) may comprise digital electronic containers that securely contain corresponding digital electronic control information. Such containers may, for example, use cryptographic techniques. In other examples, the organizational structure(s) may define associations with other electronic control information. The other electronic control information may be delivered independently over the same or different communications path used to deliver the organizational structure(s).

In one example, the steganographic techniques employed may involve applying the organizational structure information in the form of high frequency "noise" to an analog information signal. Spectral transforms may be used to apply and recover such steganographically-encoded high frequency "noise." Since the high frequency noise components of the information signal may be essentially random, adding a pseudo-random steganographically encoded control signal component may introduce substantially no discernible information signal degradation, and may be difficult to strip out once introduced (at least without additional knowledge of how the signal was incorporated, which may include a shared secret).

In accordance with another aspect provided by the invention, a steganographic encoding process analyzes an information signal to determine how much excess bandwidth is available for steganographic encoding. The steganographic encoding process may use variable data rate encoding to apply more control information to parts of an information signal that use much less than all of the available communications channel bandwidth, and to apply less control information to parts of an information signal that use nearly all of the available communications channel bandwidth.

In accordance with still another aspect provided by the invention, multiple organizational structures may be steganographically encoded within a given information signal. The multiple organizational structures may apply to different corresponding portions of the information signal, and/or the multiple organizational structures may be repetitions or copies of one another to ensure that an electronic appliance has "late entry" and/or error correcting capability and/or can rapidly locate a pertinent organizational structure(s) starting from any arbitrary portion of the information signal stream.

In accordance with yet another aspect provided by this invention, an organizational structure may be steganographically encoded within a particular portion of a content-carrying information signal to which the organizational structure applies--thereby establishing an implicit correspondence between the organizational structure and the identification and/or extent and/or semantics of the information content to which the organizational structure applies. The correspondence may, for example, include explicit components (e.g., internally stated start/end points), with the storage or other physical association determined by convenience (i.e., it may make sense to put the organizational structure close to where it is used, in order to avoid seeking around storage media to find it).

In accordance with yet another aspect provided by this invention, pointers can be steganographically encoded into parts of an information signal stream that has little excess available bandwidth. Such pointers may be used, for example, to direct an electronic appliance to portions of the information signal stream having more available bandwidth for steganographic encoding. Such pointers may provide improved steganographic decode access time--especially, for example, in applications in which the information signal stream is stored or otherwise available on a random access basis.

#### DRAWING DESCRIPTION:

#### BRIEF DESCRIPTION OF THE DRAWINGS

These and other features and advantages provided by this invention may be better and more completely understood by referring to the following detailed description of presently preferred example embodiments in conjunction with the drawings, of which:

FIG. 1 shows a virtual distribution environment providing steganographic encoding of digital rights management control information;

FIGS. 1A-1E show example electronic appliances embodying aspects of this invention;

FIG. 2 shows an example of how electronic control information can be steganographically encoded within an image;

FIG. 3 shows an example rights management component providing a steganographic decoding function;

FIG. 4 shows an example of how steganographically encoded electronic control signals can be extracted and used for digital rights management;

FIGS. 5A-5D show example techniques for enforcing steganographically encoded rights management control information;

FIGS. 5E-5F show example "end to end" protected distribution systems provided in accordance with the invention;

FIG. 6 shows an example of multiple sets of digital rights management control information steganographically encoded onto different parts of the same information signal stream;

FIG. 7A shows an example detailed steganographic encoding process;

FIG. 7B shows an example detailed steganographic decoding process;

FIG. 8 shows an example frequency domain view of an example steganographic signal encoding technique;

FIG. 9 shows an example use of a variable steganographic encoding rate to avoid exceeding channel bandwidths;

FIGS. 10 and 10A show how steganographically encoded pointers can be used to minimize access times to control signals steganographically encoded onto information signal streams available on a random access basis;

FIG. 11 shows an example steganographically encoded organizational structure;

FIG. 12 shows an example electronic appliance architecture having electronic rights management capabilities based at least in part on steganographically encoded control information;

FIGS. 13 and 13A show example control steps that may be performed by the FIG. 12 appliance;

FIG. 14 shows an example steganographic refresh arrangement; and

FIGS. 15A-15F show example distribution systems using steganographic encoding of rights management control information along at least one leg of an information distribution path.

#### DETAILED DESCRIPTION:

#### DETAILED DESCRIPTION OF PRESENTLY PREFERRED EXAMPLE EMBODIMENTS

FIG. 1 shows an example Virtual Distribution Environment (VDE) 50 employing steganography to deliver electronic digital rights management control information over an insecure (e.g., analog) communications channel.

In this example, a provider 60 delivers an information signal 70 to multiple electronic appliances 100(1), . . . , 100(N). In this particular example, provider 60 is shown as being a television broadcaster that delivers an analog television information signal 70 over a wireless or cable communications path, and appliances 100(1), . . . , 100(N) are shown as being home color television sets 106. As made clear by FIGS. 1A-1E, the present inventions may be used by a variety of different types of electronic appliances 100 receiving a variety of different types of information signals via a variety of different types of communications channels.

In the FIG. 1 example, provider 60 steganographically encodes electronic rights management control information 126 into the information signal 70. This control information 126 is represented in this diagram as a traffic light because it may define permitted and/or required operation(s), and consequences of performing or failing to perform such operations. For example, control information 126 could specify that a viewer or class of viewers has permission to watch a particular program, is forbidden to watch a program, or may watch a program only under certain conditions (for example, based on paying a certain amount, being over a certain age, etc.). In this example the control information 126 is shown as being packaged within an electronic "container" 136. Container 136 (which in at least one example is provided by steganographic encoding techniques) is used to protect the integrity of the control information 126.

The provider 60 encodes the electronic rights management control information 126 onto information signal 70 using steganographic techniques that make the control information both:

substantially invisible, and

substantially indelible.

The control information 126 is substantially indelibly encoded because, in this example, it is substantially inextricably intertwined with the television images and/or sound--and can't easily be eliminated from information signal 70 without destroying the images, sound or other information carried by the information signal. For example, steganographically encoding rights management control information will generally survive compression and decompression of a digitized analog signal, and will also survive repeated analog/digital/analog conversion sequences.

Even though the steganographically encoded control information 126 is substantially indelible, the television viewer is not bothered by the steganographically encoded information because the steganographically encoded rights management control information is, in this example, also encoded substantially invisibly. In fact, the viewer may not be able to see the steganographic control information at all--and it may have no effect whatsoever on his or her viewing experience (other than in terms of the effect it has on associated rights management processes). The control information 126 is shown in dotted lines on the FIG. 1 screens of television sets 106 to emphasize that the control information is substantially inextricably intertwined with the television images and/or sounds--and yet can't really be seen or noticed by the television viewer.

FIG. 2 shows an example of how digital control information 126 may be encoded within an image 128 so that, in one particular example, it is both

substantially invisible and substantially indelible. In this specific image context, for example, "substantially invisible" may refer to the characteristic of the encoded control information as not substantially interfering with or adversely affecting the viewer's experience in viewing image 128 or otherwise using the content carried by the information signal 70 and/or that it is difficult to detect using various types of signal processing techniques, for example. For example, invisibility can be a measurable quantity (measured in a number of processor instructions, such as MIPS years, for example), and can be related to signal processing as opposed to the naked eye. In this context, "substantially indelible" can mean, for example, that the encoded digital control information is substantially inextricably intertwined with the content information, making it difficult for example to strip out the encoded digital control information without also damaging or degrading the content. Degree of indelibility may, for example, be measured by the number of processor instructions required to strip the information out.

FIG. 2 shows that a slight rearrangement of picture element configuration in a small portion of image 128 is one way to steganographically encode electronic control information into the image to provide a substantially indelible, substantially invisible encoding. This encoding may be unnoticeable to the viewer, and yet it may be difficult to strip out or eliminate without also damaging the image. Steganographically encoding digital control information into the information signal 70 may effectively merge, from a practical standpoint, the digital control information with the other information carried by the signal (for example, television programming or other content). The steganographic techniques make it difficult for someone to intentionally or unintentionally eliminate the encoded control information without damaging the content, but may (in one example) nevertheless hide the encoded control information so that it does not unduly detract from the content.

Since indelibility of the steganographic encoding provides persistence, indelibility may be more important than invisibility in at least some applications. For example, it may be desirable in some applications to use a shared secret to decode and then remove the steganographically encoded control information 126 before presenting the information signal (or its content) to the user. The steganographically encoded information need not be particularly invisible in this scenario. Even though someone with knowledge of the shared secret can remove the steganographically encoded information, it may nevertheless remain substantially indelible to anyone who doesn't know the shared secret required to remove it.

#### Organization Structures

FIG. 1 shows that control information 126 may be packaged within one or more organizational structures such as secure digital containers 136. Containers 136 may be, for example, of the type described in the Ginter et al. patent specification in connection with FIGS. 17-26B. The organizational structure(s) may identify, implicitly or explicitly, the content the electronic controls apply to. The organizational structure(s) may also define the extent of the content, and semantics of the content.

The organizational structure(s) may be encoded in such a way that they are protected for purposes of secrecy, authenticity and/or integrity. The employed steganographic technique may provide such protection, or another security technique may be used in conjunction with steganography to provide a desired or requisite degree of protection depending on the application. Containers 136 may, for example, use mathematical techniques called "encryption" that help guarantee the integrity and/or secrecy of the control information 126 they contain.

#### Example Rights Management Component

Each of the FIG. 1 example appliances 100 may include a electronic digital rights management component 124. Rights management component 124 may, for example, comprise one or more tamper-resistant integrated circuit "chips". Components 124 may, for example, be of the general type described in detail at FIG. 9 and following of the Ginter et al. patent specification. Briefly, Ginter et al. describes a Virtual Distribution Environment ("VDE") including multiple electronic appliances coupled together through a communications capability.

Each electronic appliance has such a secure, tamper-resistant "protected processing environment" in which rights management processes may securely take place. The Virtual Distribution Environment delivers digital control information to the protected processing environments by packaging the control information within secure electronic digital containers. This delivered control information provides at least part of the basis for performing electronic rights management functions within the protected processing environments.

The ability to securely deliver digital control information to such protected processing environments as embodied with components 124 is important at least because it increases flexibility and enhances functionality. For example, different digital control information can be delivered for the same or different electronic content. As one specific example, one set of rules may apply to a particular television program, another set of rules might apply to a particular film, and a still different set of rules could apply to a particular musical work. As yet another example, different classes of users of the same electronic content can receive different control information depending upon their respective needs.

Rights management components 124 are able to steganographically decode the control information 126 carried by the information signal 70. Components 124 use the decoded control information 126 to electronically manage rights. For example, components 126 may use the decoded control information 126 to control how the images and/or sound carried by information signal 70 may be used.

In one example, digital rights management component 124 may comprise or include one or more integrated circuit chips as shown in FIG. 3. The FIG. 3 example rights management component 124 includes an analog-to-digital converter 130, a steganographic decoder 132, and a rights management processor 134. Rights management processor 134 may include or comprise a protected processing environment 138 as described in Ginter et al. FIGS. 8-12, for example, providing a tamper-resistant execution environment for effecting the operations provided by electronic controls 126. Rights management component 124 may also include a steganographic encoder and a digital-to-analog converter (not shown).

The analog-to-digital converter (ADC) 130 shown in FIG. 3 takes the incoming information signal 70 and--if it is in analog form--converts it to a digital signal (see FIG. 4, step "A"). Steganographic decoder 132 obtains the digital control information 126 from the resulting digital signal (FIG. 4, step "B"). As mentioned above, digital control information 126 may define permitted and/or required operation(s) on the content carried by signal 70, and may further define consequences of performing and/or failing to perform such operations. Rights management processor 134 may manage these rights and/or permissions and associated consequences (FIG. 4, step "C").

#### Example Electronic Appliances

The present inventions may be used with all sorts of different kinds of electronic appliances 100 each of which may include a rights management component 124. FIGS. 1A-1E show various example electronic appliances 100 embodying aspects of the present invention. For example:

FIG. 1A shows an example media player 102 capable of playing Digital Versatile Disks (DVDs) 104 on a home color television set 106. For example, media player 102 may provide analog output signals to television set 106, and may also process digitized video and/or audio analog signals stored on optical disk 104. Rights management component 124A provides digital rights protection based on steganographically encoded controls 126.

FIG. 1B shows an example set top box 108 that can receive cable television signals (for example, via a satellite dish antenna 110 from a satellite 112) for performance on home television set 106. Set top box 108 shown in FIG. 1B may receive television signals from antenna 110 in analog scrambled or unscrambled form, and provide analog signals to television 106. Rights management component 124B provides digital rights protection based on steganographically encoded controls 126.

FIG. 1C shows an example radio receiver 114 that receives radio signals and

plays the radio sound or music on a loud speaker 116. The radio receiver 114 of FIG. 1C may receive analog radio signals, and provide analog audio signals to loud speaker 116. Rights management component 124C provides digital rights protection based on steganographically encoded controls 126.

FIG. 1D shows an example video cassette recorder 118 that can play back video and sound signals recorded on a video cassette tape 120 onto television 106. In FIG. 1D, the video tape 120 may store video and audio signals in analog form, which VCR 118 may read and provide to television 106 in analog form. Rights management component 124D provides digital rights protection based on steganographically encoded controls 126.

FIG. 1E shows an example television camera that can capture video images and produce video signals for recording on a video cassette tape 120 and play back on television set 106. The FIG. 1E camcorder 122 may generate analog video and audio signals for storage onto video tape 120, and/or may provide analog signals for processing by television 106. Rights management component 124E provides digital rights protection based on steganographically encoded controls 126.

#### Example Rights Management Enforcement Techniques

Different rights holders want different types of rights management and control. For example, some rights holders may be completely satisfied with a relatively simple "copy/no copy/one copy" rights management control model, whereas other rights holders may desire a richer, more complex rights management scheme. The present inventions flexibly accommodate a wide variety of electronic rights management techniques--giving rightsholders extreme flexibility and programmability in defining, for example, commerce and rights management models that far exceed the simple "copy/no copy, one copy." Assuming a closed appliance, that is, one lacking at least an occasional connection to a payment method (e.g., Visa, MasterCard, American Express, electronic cash, Automated Clearinghouses (ACHs) and/or a Financial Clearinghouse that serves as the interface for at least one payment method), the following are non-limiting examples of steganographically encoded rights controls and associated consequences that can be accommodated by the present invention:

Limiting use of a given property to a specified number of times this property can be used on a given appliance;

Prohibiting digital to analog and analog to digital conversions;

Ensuring that one analog or digital appliance will communicate the protected property only to another appliance that is also VDE enabled and capable of enforcing the controls associated with that property;

Time-based rental models in which a consumer may "perform" or "play" the property an unlimited number of times in a given interval (assuming the appliance has a built-in secure time clock, can operatively connect itself to such a clock, or otherwise receive time from a reliable source);

Enforcing an expiration date after which the property cannot be performed (also assuming access to a reliable time source);

Associating different control sets with each of several properties on a single physical media. In one example, a "trailer" might have unlimited copying and use associated while a digital film property may have an associated control set that prevents any copying;

Associating multiple control sets with a given property regardless of media and whether the appliance is closed or has an occasionally connected communications "backchannel."

An even more flexible and diverse array of rights controls and associated consequences are enabled by the present inventions if at least one appliance is connected to some form of communications "backchannel" between the appliance and some form of payment method. This backchannel may be a telephone call, the use of a modem, a computer data network, such as the Internet, a communications channel from a settop box to the head end or some other point on a cable TV

distribution system, or a hybrid arrangement involving high bandwidth distribution of analog properties with a slower return channel, a phone line and modem--just to name a few examples. Non-limiting examples of such more rights controls and associated consequences enabled by the present invention include the following:

Associating with a given property in analog format new, independently delivered controls obtained from a rightsholder or other authorized source;

A broad range of usage-based pricing models, including pay-per-view or pay-per-use;

Creating permissions enabling excerpting of properties in analog formats, maintaining persistent control over those excerpts, and charging for those excerpts;

Pay-per-use models in which a customer pays a specified price for each use of the property and/or different unit prices depending on the number of uses. In one example, the customer might pay \$3.99 for the first viewing and \$2.99 for each subsequent viewing; and,

Controls that prevent an analog property being converted to digital format and then being transmitted or communicated except in a container with controls and/or with a pointer to a source of controls, that apply in a digital environment.

FIGS. 5A-5D show some examples of how rights management component 124 can enforce steganographically encoded digital rights management controls.

In the FIG. 5A example, rights management component 124 controls an on/off switch 140 based on steganographically encoded electronic controls 126. Component 124 turns switch 140 on (for example, to allow the analog television signal to pass to television set 106) when electronic controls 126 permit, and otherwise opens (turns off) switch 140 to prevent the analog signal from reaching the output.

In a more secure-example, the incoming analog signal is scrambled, and the FIG. 5A on/off switch 140 is replaced by a FIG. 5B descrambler 142 of conventional design. The descrambler 142 descrambles the analog input signal to provide a descrambled output under control of rights management component 124. Rights management component 124 allows descrambler 142 to descramble the analog signal only under conditions specified by electronic controls 126 that the component 124 obtains from the analog input signal. Scrambling the analog signal gives the rights management component 124 a relatively secure way of enforcing electronic controls 126--since the rights management component can prevent the descrambler from operating unless conditions set by the controls are satisfied. The rights management function and the descrambling function may be integrated into a single component in which the descramble and decrypt functions of the rights management component are essentially serving the same function, but may still be distinct to account for specialized approaches to descrambling that may not be sufficiently strong or interoperable with other environments to use generally. If they are separate components, the data path between them should be protected (for example, by ensuring that both components are in a tamper resistant enclosure, or using secure authentication and key exchange to send the descrambling sequence to the descrambler).

FIG. 5C shows how digital certificates may be used to enforce steganographically encoded electronic controls 126. In this example, appliance 100A outputs content to another appliance 110D only if appliance 100D has a rights management component 124D that can enforce the electronic controls 126. In this example, there may be a "handshake" between the content supplying appliance 100A and the content receiving appliance 100D sufficient to ensure the content supplying appliance that the content receiving appliance will enforce the electronic controls 126. For example, the supplying appliance 100A's rights management component 124A may require the receiving appliance 100D's rights management component 124D to present a digital certificate 199 attesting to the fact that the receiving appliance 100D has a rights management component 124 fully capable of securely enforcing electronic controls 126. Receiving appliance 110D could present this digital certificate 199 by

steganographically encoding it within an analog signal it provides to the supplying appliance over an analog signal channel for example (the analog signal channel could be the same one the supplying appliance will use to deliver the steganographically encoded content). If a digital channel is available, the handshake can be over a digital link between the two appliances using, for example, secure authentication techniques disclosed in Ginter et al. and/or for example in Schneier, Applied Cryptography (2d Ed. Wiley 1996) at page 52 et seq.

FIG. 5D shows that rights management component 124A can enforce electronic controls 126 by marking the content through "fingerprinting" and/or "watermarking" prior to releasing the content to a device that doesn't have a rights management component 124. See Ginter et al. patent specification, FIGS. 58A-58C. Such fingerprinting could involve using steganographic techniques to fingerprint the content. For example, a movie delivered using "conventional" containers as disclosed in Ginter et al. could use steganographically encoded containers "on the way" to the display device. Furthermore, it could include the identity of the user, etc. as well as the control information appropriate for the device. Another case could be text sent to a printer, using different steganographic encoding techniques such as line and/or character shifting.

#### End to End Protection

FIGS. 5E-5F illustrate how the persistent association with content provided by steganographically encoded electronic rights management control information 126 provides "end to end" protection within an arbitrary information signal distribution system--irrespective of the processes the information signal is subjected to as it travels to its final destination.

FIG. 5E shows an example of how the present inventions can be used to maintain end-to-end rights management protection over content initially distributed in an analog signal format. FIG. 5F shows an example of how the present invention can be used to maintain end-to-end rights management protection over content initially distributed in digital form.

In the FIG. 5E example, an analog signal transmission site (e.g., a radio or television broadcaster) transmits an analog signal A steganographically encoded with an organizational structure 136 including electronic controls 126. This analog signal A may be received by an electronic appliance 100A having a rights management component 124A as described above. Appliance 100A may, for example, convert the signal into digital and/or digitized format, and store the digitized version of the signal onto a digital storage medium 104. Electronic appliance 100A may play back the recorded digitized signal, convert the signal back to analog form, and deliver the analog signal A to a further electronic appliance 106B. In this example, electronic appliance 106B also has a rights management component 124B.

The steganographic techniques provided by the present invention ensure that the electronic controls 126 persist in the signal A delivered from appliance 100A to appliance 106B--and from appliance 106B to still other appliances. Because of the substantial indelibility characteristics of the steganographically encoded control information 126, this information persists in the signal as stored on recording medium 104, in copies of the recorded signal produced by replaying the medium, and in further downstream versions of the signal.

This persistence will, for example, survive conversion from analog to digital format (e.g., sampling or "digitizing"), storage, and subsequent conversion from digital to analog format. For example, because the steganographically encoded control information 126 is substantially indelibly, substantially inextricably intertwined and integrated with the information signal A, the digitized version of the information signal that appliance 100A records on medium 104 will also contain the steganographically encoded control information 126. Similarly, when appliance 100A plays back the recording from medium 104, it will reproduce information signal A along with the steganographically encoded control information 126. The steganographically encoded control information 126 thus persists irrespective of digitization (or other processing) of signal A. In some cases, lossy compression techniques used on the data may remove high frequency noise--thereby potentially damaging the steganographic channel. When these lossy compression techniques are used or may

be encountered, the steganographic encoding function should be matched to the compression algorithm(s) using conventional signal analysis techniques to avoid this consequence.

Similarly, appliance 106B may output further copies or versions of signal A in analog form and/or digital form. Because of its inherently persistent characteristics, the steganographically encoded control information 126 will be present in all subsequent versions of the signal outputted by appliance 106B--be they in analog format, digital format, or any other useful format.

Degrading a digital signal carrying control information is fatal--the rights management system typically may no longer function properly if even a single bit is altered. To avoid this, the preferred embodiment provides redundancy (repeating pointers and the organizational structures and/or any control information incorporated into the organizational structures), and also uses conventional error correction coding such as, for example, Reed-Solomon (or similar) error correcting codes. Additionally, because the steganographically encoded control information 126 is substantially inextricably intertwined with the desired content carried by information signal A, any process that degrades the steganographically encoded control information 126 will also tend to degrade the information signal's desired content. Although the steganographically encoded information may degrade (along with the content) in multi-generation "copies" of the signal, degraded copies may not be commercially significant since the information content of the signal will be similarly degraded due to the substantially inextricable intertwining between the steganographically encoded control information 126 and the content carried by signal A. The refresh circuit shown in FIG. 14 with appropriate error correcting capabilities is one way to prevent the steganographically encoded information from being degraded even if the rest of the information the signal carries becomes degraded.

The FIG. 5F example shows content being initially distributed in digital form over a network to an electronic appliance 100J such as a personal computer. Personal computer 100J may convert the digitally delivered content to an analog signal A for distribution to other appliances 106B, 100A. Personal computer appliance 100J may include a rights management component 124J that ensures, based on controls 126, that appliance 100J does not release a version of the content associated with controls 126 that is not protected by the controls. In this example, rights management component 124J is capable of steganographically encoding the analog signal A with the control information 126 (e.g., it may perform the processes shown in FIG. 7A below). Rights management component 124J enforces controls 126, at least in part, by ensuring that any analog version of the content associated with controls 126 is steganographically encoded with those controls. Further "downstream" appliances 106B, 100A may each include their own rights management component 124 for use in interacting with steganographically encoded controls 126.

#### Example Control Information

FIG. 6 shows that a particular information signal 70 may be encoded with many different containers 136 and associated rights management control sets 126. For example, different portions of an information signal 70 may be associated with different control information 126. In this example of a movie 270:

a first "trailer" 272 may be associated with control information 126(1),

a second trailer 274 may be associated with control information 126(2),

a title section 276 may be associated with control information 126(3),

the first five minutes of the movie may be associated with control information 126(4), and

the rest of the movie may be associated with control information 126(5).

Control information portions 126(1), 126(2), 126(3), 126(4) and 126(5) may all be different. For example, control information 126(1) may permit the user to copy trailer 272, whereas control information 126(4) may prohibit the user from copying the first five minutes 278 of the film.

As shown in FIG. 6, multiple, identical copies of control information 126(5) may be steganographically encoded onto the information signal 70. For example, control information 126(5) could be encoded once per minute onto the rest of movie 280. This redundancy allows a media player 102 or other electronic appliance 100 to rapidly obtain a copy of the control information 126(5) no matter where the user begins watching or playing the movie 270, and also helps ensure that transmission errors will not prevent the rights management component 124 from recovering at least one "good" copy of the organizational structure.

#### Example Steganographic Encoding and Decoding Processes

FIGS. 7A and 7B show example overall steganographic encoding and decoding processes, respectively. The FIG. 7A process may be used to steganographically encode digital control information onto an analog signal, and FIG. 7B performs the inverse operation of steganographically decoding the control information from the analog signal. Generally, the FIG. 7A process may be performed at a supply point, and the FIG. 7B process may be performed at a usage point. An electronic appliance 100 can be both a supply point and a usage point, and so it may perform both the FIG. 7A process and the FIG. 7B process.

Referring to FIG. 7A, the analog information signal 70 inputted to the steganographic encoding process may be any sort of information signal such as, for example, the analog signal shown in Graph A1. A conventional analog-to-digital conversion block 402 may be used, if necessary, to convert this analog input signal to a digitized signal (see Graph A2). A spectral transform block 404 may then be used to transform the digitized information from the time domain to the frequency domain. Spectral transform block 404 may be any conventional transformation such as, for example, a Fast Fourier Transform (FFT) or a Walsh Transform. An example of the resulting spectral information is shown in the A3 graph.

A steganographic encode block 406 may be used to steganographically encode digital control information 126, in clear text form and/or after encryption by a conventional digital encryption block 414 based on an encryption key Key.sub.s. Steganographic information can be combined with a pseudo-random data stream (e.g. exclusive-or'd into the output of a DES engine)--in effect shuffling around the noise in the signal rather than replacing noise with the signal, per se. When protection is desired, the values in the pseudo-random stream can be protected by encryption (e.g. the key that initializes the DES engine should be protected). When the steganographic channel is "public" (e.g., unencrypted), the stream should be readily reproducible (e.g. by using one of a preset collection of values shared by every device). A small portion (a "public header"--see Ginter et al.) is always detectable using a shared preset value (that does not need to be protected, distinguishing it from the private header keys), may be provided to ensure that the rights management technology can be activated properly. Since the rights management component 124 at the receiving side needs to know how to descramble the signal, there normally will be an indication in the "public header" that names a key that will be used to unlock the private header (and so on, as described, for example, in Ginter et al.). Some publicly available, agreed upon preset values may be used to extract the "public header" information from the steganographically encoded channel.

Steganographic encode block 406 may be any conventional steganographic encoding arrangement capable of steganographically encoding a digital signal onto information signal 70. Steganographic encode step 406 may be based on a key K.sub.c --allowing the same basic steganographic encoding and decoding transformations to be used by a wide variety of different appliances while still maintaining individuality and secrecy through the use of different steganographic keys.

In one example, the steganographic encoding step 406 may introduce the (encrypted) digital control information into the high frequency spectrum portion of the spectrally transformed information signal 70. The spectrally transformed signal with steganographic encoding is shown in the FIG. 7A Graph A4, and is shown in more detail in FIG. 8. As FIG. 8 shows, the steganographic encoding may affect the higher order frequency components of the spectrally transformed signal (see dotted perturbations in the fourth, fifth, sixth,

seventh and eighth order components in FIG. 8). The steganographic encoding may add to and/or subtract from the amplitudes of these higher order components. The effect of introducing high frequency steganographically encoded signal components may be to mask the steganographic encoding within the random high frequency noise inherently provided within information signal 70--thereby providing substantial invisibility and substantial indelibility.

The amount of amplitude modification performed by steganographic encode step 406 may be limited in this example to ensure that the resulting steganographically encoded signal does not exceed the available channel bandwidth. See, for example,

J. Millen, "Covert Channel Capacity," IEEE Symposium on Security and Privacy (1987).

R. Browne, "An Entropy Conservation Law for Testing the Completeness of Covert Channel Analysis," Fairfax 94, pp 270-281 (1994).

Moskovitz et al., "The Channel Capacity of a Certain Noisy Timing Channel," IEEE Trans. on Information Theory v IT-38 no. 4, pp. 1330-43, (1992).

Venkatraman, et al., "Capacity Estimation and Auditability of Network Covert Channels," Oakland 95, pp. 186-298.

The following equations show the relationship between total bandwidth, bandwidth available for steganographic encoding, and the data rate of the steganographically encoded signal: ##EQU1##

where  $\Delta t = t_{n+1} - t_n$ , and

B is a function of time in bits/second.

In the above expressions, the function S corresponds to an area under a curve resulting from the product of B (bandwidth) and t (time). The parameter delta t refers to the "granularity" of the analog-to-digital conversion (i.e., 1/sampling rate).

FIG. 9 shows an example plot of information signal bandwidth versus time. The total bandwidth available is limited by the bandwidth of the transmission channel--including the bandwidth of the storage medium (if any) used to deliver the signal, and the bandwidth of the reproduction equipment. Since the total bandwidth depends on the inherent characteristics of the transmission channel used to communicate information signal 70, it is typically a fixed constant. FIG. 9 shows that the bandwidth actually used by the information signal 70 typically varies with time. For example, although somewhat counterintuitive, the more complex an image, the more noise is typically available for "shuffling around" to create a steganographic channel. Of course, this isn't always true--a highly intricate geometric pattern may have very little noise available for encoding, and a simple picture of a cloud may have a great deal of noise available.

Steganographic encode block 406 can use an encoding rate and characteristic that ensures the steganographically encoded signal bandwidth doesn't exceed the total bandwidth available in the communication channel. Typically, the amount of bandwidth available for steganographic encoding may be on the order of on the average of 0.1% of the total transmission channel bandwidth--but as mentioned above, this bandwidth available for steganographic encoding may be unequally distributed with respect to time within the information signal stream 70 and may depend on the content of the information signal.

In this example, steganographic encode block 406 analyzes the content (e.g., by performing statistical weighted averaging), and provides a responsive variable steganographic encoding rate. For example, steganographic encoding block 406 can use a high data rate during example time periods "II" and "IV" in which the information signal 70 has characteristics that allow high steganographic rate encoding without the resulting signal exceeding the available overall channel bandwidth. Encoding block 406 can use a low data rate during time periods "I" and "III" in which the information signal 70 has characteristics that do not allow high data rate steganographic encoding without exceeding available

overall channel bandwidth. Steganographic encoding block 406 may use any number of different variable rates to accommodate different relationships between information signal 70 characteristics and available channel bandwidth.

Referring again to FIG. 7A, the steganographically encoded spectral information outputted by steganographic encode block 406 may be subjected to an inverse spectral transform 408. Inverse spectral transform 408 in this example may perform the inverse of the transform performed by step 404--outputting a version of the digitized time domain signal shown in Graph A2 but now bearing the steganographically encoded information (Graph A5). The digital control information steganographically encoded by block 406 may be substantially indelible and substantially invisible with respect to the Graph A5 signal--that is, it may be very difficult to eliminate the steganographically encoded information and it may also be very difficult to discern it.

This signal may be further scrambled and/or encrypted (e.g., used on a scrambling and/or encryption key Key.sub.d) before being converted to analog form (shown in Graph A6) by a conventional digital-to-analog conversion block 412 (if necessary). Signal scrambling may be independent of steganographically encoded control information. For example, a good way to support existing devices is to not scramble the signal, and to use legislative means to ensure that each new device manufactured is equipped with rights management technology. Scrambling/encrypting of content, can be used to enforce use of rights management. If legislative means can enforce the use of rights management technology, encryption or scrambling of content may not be necessary (although a decision to provide cryptographic protection for the control information is independent of this factor and must be evaluated in light of protecting the rights management system). Rights holders can choose an enticement technique(s) based on their business model(s). The benefit of scrambling is that it provides technical means for enforcing rights management. The benefit of unscrambled content is support of hundreds of millions of devices in the installed base--with the promise that new devices (potentially including computers) will enforce the control information even though they don't "have to" from a technical perspective.

The resulting steganographically encoded information signal 70 may then be transmitted over an insecure communications channel. Digital-to-analog conversion step 412 may be omitted if a digital communications channel (e.g., an optical disk, a digital satellite link, etc.) is available to deliver the signal.

FIG. 7B shows an example inverse process for recovering digital control information 126 from the steganographically encoded information signal 70. In this recovery example, the steganographically encoded analog signal is converted to a digitized signal (if necessary) by an analog-to-digital conversion step 402' and decrypted/descrambled (if necessary) by a decryption/descrambling block 422' to yield a facsimile of the inverse spectral transform block 408 output shown in FIG. 7A. In this FIG. 7B example, the analog-to-digital conversion block 402' is the inverse operation of FIG. 7A, block 412, and the decrypt/descramble block 422' is the inverse of the FIG. 7A scramble/encrypt block 410.

The resulting digitized signal provided by FIG. 7B block 422' is spectrally transformed by step 404' (this may be the same spectral transform used in FIG. 7A, block 404) to yield a steganographically encoded spectral signal A3. Steganographic decode block 424 may perform the inverse operation of the FIG. 7A steganographic encode block 406 based on the same steganographic key Key.sub.c (if a key-based steganographic encoding/decoding transformation is used). The output of steganographic decode block 424 may be decrypted by block 426 (the inverse of FIG. 7A encrypt block 414 based on key Key.sub.s) to provide recovered digital control information 126. The resulting control information 126 may be used for performing electronic rights management functions. Required keys may be delivered in containers and/or using the key distribution techniques and device initialization approaches disclosed in Ginter et al., for example.

#### Example Control Information Arrangements

In a further example shown in FIGS. 10 and 10A, steganographic encode block 406

may encode control information organizational structures such as secure containers (see Ginter et al., FIGS. 17-26B and associated text) during times when the content bandwidth is low relative to the total available bandwidth (see FIG. 10 regions II and IV), and may not attempt to encode such organizational structures during times when the content bandwidth is high relative to the total available bandwidth (see FIG. 10, regions I, III). In this way, steganographic encode block 406 may maximize the total bandwidth use without causing the steganographically encoded signal to exceed available bandwidth. As an optimization for certain applications, steganographic encode block 406 may encode "pointers" or other directional information into the information signal 70 during times when the content is such that it doesn't allow high data rate steganographic encoding of organizational structures 136. Multiple pointers and multiple "pointed to" locations can also help provide redundancy.

This particular FIG. 10 example involving steganographic encoding of pointers 800 may be especially suited for content delivery or presentation on random access storage media such as optical disks. Using such random access media, a content handling device may be able to rapidly "seek" to the place where an organizational structure is stored at a higher recorded bandwidth and then read the organizational structure at this higher bandwidth (See FIG. 10A). For these example arrangements, steganographic encode block 406 in this example encodes, during periods when the content is such that it is not possible to steganographically encode organizational structures, pointers 800 that direct the content handling device to one or more places where the organizational structure appears in the content stream. In one example, pointers 800 might encode the location(s) on a storage medium (e.g., an optical disk 104--see FIG. 10A) at which the closest organizational structure is stored.

An optical disk player 102 with random access capability may "seek" to the place at which the closest organizational structure 136 is stored on the disk 104, and rapidly read the organizational structure off of the disk in less time than might be required to read an organizational structure that steganographic encode block 406 encodes at a lower data rate during times when the content bandwidth occupies most of the available channel bandwidth. In such arrangements, the process of reading a pointer 800, "seeking" to a position on the medium specified by the pointer, and then reading an organizational structure 136 steganographically encoded at a high data rate may provide overall faster access times than if the organizational structure was itself encoded at a lower data rate within the parts of the information signal stream used in this example to encode only pointers.

FIG. 11 shows an example organizational structure 136 suitable for steganographic encoding similar to that shown in FIG. 17 of the co-pending Ginter et al. application. In the case of container 136 with controls for an analog property, the organizational structure may include one or more permissions records 136d providing control sets 136e providing electronic controls especially for an analog device(s). The permissions record 136d may also provide a reference 136f at least one location or other external source for additional controls. This reference may be to an Internet "Uniform Resource Locator" (URL), for example. The organizational structure 136 may optionally include a content block 136g providing digital content subject to the controls. In this example, organizational structure 136 is encased in a protective "wrapper" 136x provided by the steganographic technique used to encode the organizational structure 136, digital encryption techniques, and/or a combination of the steganography and encryption. This protective wrapper 136x is used to ensure that the organizational structure 136 cannot be tampered with and maintains its integrity. Wrapper 136x may also provide a degree of confidentiality if required.

#### Detailed Example Electronic Appliance Architecture

FIG. 12 shows an example detailed internal architecture for an example electronic appliance 100 such as optical disk player 102. In this specific example, rights management component 124 may be a tamper-resistant integrated circuit including internal microprocessor 200, flash memory 202 and cryptographic engine 204 (see Ginter et al. FIGS. 9-15B and associated text for a more detailed internal view of an example tamper-resistant rights management component 124 and a "protected processing environment" 138 it provides).

A main system bus 206 may couple rights management component 124 to a main system microprocessor 208 and various system components such as, for example, a CD-ROM decoder 210, a control and audio block 212, a video decoder 214, a digital output protection block 216, and a communications system 218. In this example, main microprocessor 208 controls the overall operations of appliance 100, with rights management component 124 performing security-related functions such as rights management and steganographic decoding.

In the FIG. 12 example appliance 102, an optical pickup 220 reads information from optical disk 104 and provides it to RF amplifier 222. RF amplifier 222 provides its output to digital signal processor (DSP) 224, which processes the output in a conventional manner and also controls the orientation of the optical disk 104 relative to optical pickup 220 via a driver 226. DSP 224 coordinates with a conventional CD-ROM decoder 210 to provide decoded digitized video and audio information. Decoder 210 operates in conjunction with a buffer memory 228, and may also cooperate with cryptographic engine 204 to ensure that any encrypted video information is decrypted appropriately.

The video output of CD-ROM decoder 210 may be decompressed by MPEG-2 video decoder 214 and applied via an NTSC and/or PAL encoder 230 to television 106. (In another example, the output could be in a non-interlaced format such as RGB rather than in interlaced formats such as NTSC and PAL.) Meanwhile, control and audio block 212 (which may operate in conjunction with its own buffer memory 232) may receive digitized audio information recorded on optical disk 204 via DSP 224 and CD-ROM decoder 210. Control and audio block 212 may provide this audio output to audio processing block 234 for output to loudspeakers 116. Control and audio block 212 may also provide an interface to the user via an infrared sensor 236 (for a remote control, for example), front-panel user controls 238 and/or an LED display 240.

In this example, security microprocessor 200 within rights management component 124 receives the digitized video and/or audio that DSP 224 reads from optical disk 104 via pickup 220 and RF amp 222. Security microprocessor 200 steganographically decodes this digitized analog information signal to recover the digital control information 126 encoded onto the information signal. Security microprocessor 200 also performs rights management functions based on the digital control information 126 it recovers. In addition, if desired security microprocessor may remove the steganographic encoding from a received digitized analog signal (since it shares a secret such as the steganographic encoding key Key.sub.c with the steganographic encoding point, it can remove the steganographic encoding) and/or steganographically encode a signal with received, augmented and/or new rights management control information.

In this example, microprocessor 200 may selectively control cryptography engine 204 to decrypt encrypted content provided by optical disk 104--thus enforcing the rights management activities provided in accordance with electronic controls 126. Security component 124 may also control digital output protection block 216 in accordance with rights management control information 126--thus, selectively permitting digital appliance 100 to output content in digital form. Rights management component 124 may take other steps (e.g., watermarking and/or fingerprinting information before releasing it) to provide a degree of copy protection and/or quality degradation to prevent or discourage someone from creating an unlimited number of high quality copies of the content of optical disk 104. Rules contained in the control information can also govern how other parts of the system behave. For example, the control information could specify that no sound can be played unless the content is paid for. Another property may specify that certain copy protection schemes should be turned on in the NTSC encoder. Still another might disable the digital outputs of the device altogether, or unless an additional fee is paid.

Rights management component 124 (protected processing environment 138) may, in this particular example, communicate over a network 144 (such as, for example, the Internet or other data communications path) with other rights management related entities, such as, for example, clearinghouses and repositories. This "back channel" allows rights management component 124 to, for example, report usage and payment information and/or to retrieve additional rights management control information 126 to augment or supplement the control information it steganographically decodes.

### Example Control Steps

FIG. 13 shows example control steps that may be performed by protected processing environment 138 (e.g., security microprocessor 200) to provide electronic digital rights protection. The FIG. 13 read/play routine 300 begins with protected processing environment 138 applying rules 126--in effect, setting the initial state in which rights management can occur (FIG. 13, block 302). Protected processing environment 138 then reads the output of CD-ROM decoder 310 (FIG. 13, block 304) and obtains steganographically encoded data from the output stream (FIG. 13 block 306). If protected processing environment 138 encounters the beginning of the control information organizational structure ("yes" exit to decision block 308), the protected processing environment performs an initialization step (FIG. 13, block 310) to begin receiving new control information 126 and then returns to block 302 to again apply current control information (FIG. 13, block 302). If, on the other hand, protected processing environment 138 encounters a continuation of an organizational structure ("yes" exit to decision block 312, FIG. 13), the protected processing environment stores the organizational structure information it has received (FIG. 13, block 314) and turns again to the apply rules step (FIG. 13, block 302).

If protected processing environment 138 encounters a pointer ("yes" exit to decision block 318), then the protected processing environment determines whether it already has received the corresponding organizational structure pointed to by the received pointer (FIG. 13, decision block 320). The protected processing environment 138 retrieves the organizational structure if it does not already have it (FIG. 13, block 322)--for example, by controlling DSP 224 to seek to the corresponding location on optical disk 104 indicated by the pointer, and by reading the organizational structure from the disk beginning at that disk location (FIG. 13, block 322).

If protected processing environment 138 has received no organizational structures or pointers ("no" exits to each of decision blocks 308, 312, 318), then the protected processing environment may determine whether there is any bandwidth available to carry control information. For example, some types of content stored on optical disk 104 may take up substantially all available channel bandwidths so that no bandwidth remains for steganographic encoding. If there is no available bandwidth for steganographic encoding ("no" exit to decision block 324), then the protected processing environment 138 may return to the "apply rules" block 302 and repeat steps 304-324 to wait until bandwidth is available for steganographic encoding. On the other hand, if there is bandwidth available and still no steganographically encoded information has appeared ("yes" exit to decision block 324, FIG. 13), protected processing environment 138 performs an error handling routine that processes the exception (FIG. 13, block 326) and determines whether the exception is critical (decision block 328). In some cases, protected processing environment 138 will continue to allow the appliance 100 to process the content, finding the error to be non-critical ("no" exit to decision block 328). An example of this would be a timer that permits playing for a period of time. In other cases (e.g., if the error conditions indicate that optical disk 104 has been tampered with), protected processing environment 138 may halt processing and return an error condition ("yes" exit to decision block 328, bubble 329).

FIG. 13A shows example steps that may be performed by the FIG. 13 "apply rules" routine 302. In this example, protected processing environment 138 may determine if it has received a complete organizational structure on which to base rights management for the rights being read from optical disk 104 (FIG. 13A, decision block 330). If the protected processing environment 138 has not received a complete organizational structure ("no" exit to decision block 330), it may disable content processing until it receives a complete organizational structure (FIG. 13A, block 331). If protected processing environment 138 has a complete organizational structure ("yes" exit to decision block 330), it determines whether it has the current organizational structure (decision block 334). If the current organizational structure is present ("yes" exit to decision block 334), the protected processing environment 138 then processes the current operation with respect to the control information embodied in the organizational structure (FIG. 13A, block 336). If the protected processing environment 138 does not have the current organizational structure ("no" exit

to decision block 334), it determines whether it has an organizational structure that has the same identification as the current organizational structure (FIG. 13A, decision block 338). The protected processing environment 138 may use that matching organizational structure as a default ("yes" exit to decision block 338, block 340). Otherwise, protected processing environment 138 disables content operations until it receives a current organizational structure ("no" exit to decision block 338, block 342).

As mentioned above, protected processing environment 138 may also perform any or all of the FIG. 7A steganographic encoding steps, and may also or alternatively remove the steganographic encoding from a signal by using a shared secret to generate a steganographic encoding stream and then subtracting that stream from the signal. Such techniques may be useful, for example, to allow protected processing environment 138 to encode new control information or to change the encoded control information. For example, the steganographically encoded control information might provide a chain of handling and control that authorizes certain protected processing environments to change some elements and add new elements to the control information 126. Protected processing environment 138 could:

steganographically decode the signal using shared secrets to obtain the control information;

modify the control information to the extent authorized by the control information;

remove the steganographic encoding from the signal based on the shared secret; and

steganographically encode the signal with the modified control information.

#### Example Refresh Capability

FIG. 14 shows another example electronic appliance arrangement including a "refresh" capability involving both steganographic decoding and steganographic encoding. In this example, electronic appliance 100 includes a steganographic decoding block 424 as described above plus an additional steganographic encoding block 406. The appliance 100 may obtain the digital control information from the content signal, and then may "refresh" the extracted information (e.g., using coding techniques, such as, for example, Reed-Solomon decoding based on Reed-Solomon codes applied to the signal by the steganographic encoding process) to correct errors and otherwise accurately recover the digital control information. The error-corrected digital control information outputted by refresh decoder 900 may be applied to a steganographic encoding circuit 406 which steganographically encodes the content signal with the refreshed control information.

The FIG. 14 refresh operation could, for example, be performed on a selective basis based on the encoded digital control information itself. For example, the control information might authorize appliance 100 to redistribute the content signal only under certain conditions--one of which is to ensure that a refreshed steganographic encoding of the same (or modified) digital control information is provided within the redistributed content signal.

#### EXAMPLES

FIG. 15A shows an example analog signal distribution arrangement 500 provided in accordance with this invention. Within arrangement 500, a steganographic encode block 400 encodes an analog information signal A with rights management control information 126 and associated organizational structure(s) 136. The steganographically encoded information signal A' is distributed by various mechanisms to user electronic appliances 100. For example, the encoded signal A' may be broadcast wirelessly over the air by a broadcaster 60A, distributed over a cable television network by a cable television head end 502, and/or distributed via a satellite communications network 504. Encoded signal A' may, during the process of being distributed, be converted from analog to digital form and back again. For example, the satellite uplink 504A may digitize signal A' before transmitting it to the satellite 504b, and the satellite downlink 504c may convert the signal back to analog before providing it to user

appliances 100. As explained above, the steganographically encoded control information 126 persists within the signal A' despite conversions between analog and digital formats.

In this example, an example set top box user appliance 108 may receive the distributed steganographically encoded analog signal A'. Set top box 108 may include a rights management component 124 as described above, and may perform rights management operations and/or processes in response to and based on steganographically encoded control information 126.

Set top box 108 in this example may output the steganographically encoded analog signal (or a facsimile of it) to additional user electronic appliances such as, for example, a television set 106, a digital optical recording device (e.g., DVD-R) 102, and/or a video tape recorder 118. Each of these additional appliances 106, 102, 118 may include a rights management component 124 that performs electronic rights management based on the steganographically encoded control information 126. Any recordings made by recording devices 102, 118 may also be steganographically encoded.

FIG. 15B shows another example analog signal distribution arrangement 510. In this example, a radio broadcaster 60B broadcasts an analog radio signal A' that is steganographically encoded with associated rights management control information 126 and associated organizational structure(s) 136. A wire network 512 such as a cable television system may similarly distribute the same or different steganographically encoded analog radio signal A'. Broadcaster 60B and/or network 512 may deliver the steganographically encoded radio signal A' to a user receiving appliance 100C such as a FM radio receiver 114. In this example, radio receiver 114 has a rights management component 124 that processes and automatically manages rights based on steganographically encoded controls 126. In this example, radio receiver 114 may (if permitted by controls 126) output steganographically encoded analog signal A' to additional appliances such as, for example, a digital recorder 102 and/or an analog recorder 514. In this example, each of appliances 100A, 100B has a rights management component 124 that electronically manages rights based on the steganographically encoded controls 126. Because the steganographically encoded controls 126 persist, recording devices 102, 514 record the steganographically encoded controls 126 in any recordings they make of signal A'. In one non-limiting example, when rights control information is encoded in steganographic sound recordings that are broadcast via radio or some other method, an airplay audit service can sample stations in a given market and identify particular properties being broadcast from "object identifier" information contained in the steganographically encoded VDE container.

FIG. 15C shows an example signal distribution arrangement 520 in which the steganographically encoded analog signal A' is initially distributed in the same manner as shown in FIG. 15A, and is then converted by an electronic appliance 100G such as a personal computer, for example, into a digital signal D. In this example, appliance 100G includes a rights management component 124 that manages rights based on steganographically encoded controls 126. Appliance 100G may convert received analog signal A' into digital form for distribution to and processing by digital appliances such as a digital high definition television 106B, a digital optical disk recorder 102, and/or a digital tape recorder 118a. In one example, the steganographically encoded control information 126 persists within the digitized signal D. In another example, appliance 100G removes the steganographic encoding from received analog signal A' and outputs a digital signal D that is "clean" and free of steganographic encoding--but is otherwise protected so that it remains persistently associated with the now-digital control information 126 (which appliance 100G may distribute, for example, within secure electronic containers 136 and digital, encrypted form. In one specific example, appliance 100G may package the received, digitized content from analog signal A' within the same digital electronic container 136 that also contains associated control information that appliance 100G steganographically decodes from analog signal A'. In another specific example, appliance 100G may distribute controls 126 independently of the digital signal D--but under circumstances in which the rights management components 124 within each of digital appliances 106B, 102 and 118A all securely associate the control information with the now-digital content.

FIG. 15D shows a similar distribution arrangement 530 for analog radio or other

audio signals. In this example, appliance 100G may include a digital radio receiver that receives analog radio signal A' and converts it into a digital information signal for distribution to digital recorders 102, 514A. As discussed above, appliance 100G may distribute the digitized analog signal A' with steganographic encoding to appliances 102, 514A--each of which includes a rights management component 124 that may recover the steganographically-encoded control information 126 and perform rights management functions based thereon. In another particular example, appliance 100G may remove the steganographic encoding from the content before distributing it in digital form--and use other techniques (such as those described in the above-referenced Ginter et al. patent specification) to provide a secure association between the now-digital content and the digital control information 126.

FIG. 15E shows yet another example distribution arrangement 540 in which digital appliances 102, 100G distribute information in digital form to a digital television 106B. For example, appliance 102 may provide digital video signals D to digital television 106B by playing them back from DVD 104. DVD player 102 may provide controls 126 within electronic digital containers 136 to digital television 106B. Digital television 106B may include a rights management component 124C that manages rights in the digital content based on digitally-provided control information 126. Similarly, computer 100G may receive digital content and associated control information 126 from a digital network 144, and provide digital video signals D and associated controls 126 to digital television 106B.

In this example, digital television 106B includes an analog output that may provide analog television signals to additional devices, such as, for example, an analog video cassette recorder 118. In this example, the rights management component 124C within digital television 106B may steganographically encode the analog television signal A with controls 126 and associated organizational structure(s) 136 before releasing the analog signal to the outside world.

FIG. 15F shows a further example arrangement 550 in which a digital appliance 100G such as a personal computer receives digital video signal D and converts it into various analog television signal formats (e.g., NTSC/PAL and/or RGB) for output to analog devices such as an analog VCR 118, an analog set top box 108 and/or an analog television set 106A. In this example, a rights management component 124G within digital appliance 100G steganographically encodes the received digital controls 126 onto the analog signal A', A" before releasing the analog signal to the additional appliances 118, 106A, 108.

While the invention has been described in connection with what is presently considered to be the most practical and preferred embodiment, it is to be understood that the invention is not to be limited to the disclosed embodiment, but on the contrary, is intended to cover various modifications and equivalent arrangements included within the spirit and scope of the appended claims.

#### CLAIMS:

What is claimed is:

1. A method including the following:

at a first apparatus, receiving a first secure digital container including a controlled item, said controlled item including a file and information steganographically encoded into said file;

at said first apparatus, receiving a first control set made up of at least one control separately from said first secure digital container;

at said first apparatus, opening said first secure digital container; and

at said first apparatus, using said first control set to control at least one aspect of access to or use of at least a portion of said controlled item, including

determining user information related to the age of a user of said first apparatus;

determining whether said user's age is equal to or greater than a threshold;

allowing said user to complete at least one access to or use of at least a portion of said controlled item if said user's age is equal to or greater than said threshold; and

blocking said user from completion of at least one access to or use of at least a portion of said controlled item if said user's age is less than said threshold.

2. A method including the following:

at a first apparatus, receiving a first secure digital container including a controlled item, said controlled item including a file and information steganographically encoded into said file;

at said first apparatus, receiving a first control set made up of at least one control separately from said first secure digital container;

at said first apparatus, opening said first secure digital container; and

at said first apparatus, using said first control set to control at least one aspect of access to or use of at least a portion of said controlled item, said use including

determining whether a conversion of at least a portion of said controlled item is authorized;

converting said portion of said controlled item if said conversion is authorized and storing said converted portion; and

failing to convert said portion if said conversion is not authorized.

3. A method as in claim 2, in which converting includes:

converting said controlled item portion from a first format to a second format.

4. A method as in claim 3, in which said first format comprises a digital format and said second format comprises an analog format.

5. A method as in claim 3, in which said first format comprises an analog format and said second format comprises a digital format.

6. A method including the following:

at a first apparatus, receiving a first secure digital container including a controlled item, said controlled item including a file and information steganographically encoded into said file;

at said first apparatus, receiving a first control set made up of at least one control separately from said first secure digital container;

at said first apparatus, opening said first secure digital container; and

at said first apparatus, using said first control set to control at least one aspect of access to or use of at least a portion of said controlled item, said use including:

gaining access to information regarding at least one aspect of a second apparatus;

determining whether transmitting said portion of said controlled item is authorized based at least in part on said second apparatus information; and

if transmitting is authorized, transmitting said portion of said controlled item from said first apparatus to said second apparatus.

7. A method as in claim 6, in which said second apparatus information includes information relating to the level of security, integrity, or copy protection present at second apparatus.

8. A method including the following:

at a first apparatus, receiving a first secure digital container including a controlled item, said controlled item including a file and information steganographically encoded into said file;

at said first apparatus, receiving a first control set made up of at least one control separately from said first secure digital container;

at said first apparatus, opening said first secure digital container; and

at said first apparatus, using said first control set to control at least one aspect of access to or use of at least a portion of said file, said use including directly or indirectly providing payment-related information to a second apparatus.

9. A method including:

at a first apparatus, receiving a first secure digital container including a controlled item, said controlled item including a file and information steganographically encoded into said file, said information including a first control set made up of at least one control;

at said first apparatus, retrieving at least a portion of said controlled item from said first secure digital container;

at said first apparatus, steganographically recovering said first control set from said controlled item; and

at said first apparatus, using said first control set to control at least one aspect of access to or use of at least a portion of said controlled item, said use including:

determining user information related to the age of a user of said apparatus;

determining whether said user's age is equal to or greater than a threshold;

allowing said user to complete at least one access to or use of at least a portion of said controlled item if said user's age is equal to or greater than said threshold; and

blocking said user from completion of at least one access to or use of at least a portion of said controlled item if said user's age is less than said threshold.

10. A method including:

at a first apparatus, receiving a first secure digital container including a controlled item, said controlled item including a file and information steganographically encoded into said file, said information including a first control set made up of at least one control;

at said first apparatus, retrieving at least a portion of said controlled item from said first secure digital container;

at said first apparatus, steganographically recovering said first control set from said controlled item; and

at said first apparatus, using said first control set to control at least one aspect of access to or use of at least a portion of said controlled item, including

determining whether a conversion of at least a portion of said controlled item is authorized;

converting said portion of said controlled item if said conversion is authorized and storing said converted portion; and

failing to perform said conversion if said conversion is not authorized.

11. A method as in claim 10, in which converting includes:

converting at least a portion of said controlled item from a first format to a second format.

12. A method as in claim 11, in which said first format comprises a digital format and said second format comprises an analog format.

13. A method as in claim 11, in which said first format comprises an analog format and said second format comprises a digital format.

14. A method including:

at a first apparatus, receiving a first secure digital container including a controlled item, said controlled item including a file and information steganographically encoded into said file, said information including a first control set made up of at least one control;

at said first apparatus, retrieving at least a portion of said controlled item from said first secure digital container;

at said first apparatus, steganographically recovering said first control set from said controlled item; and

at said first apparatus, using said first control set to control at least one aspect of access to or use of at least a portion of said controlled item, including:

gaining access to information regarding at least one aspect of a second apparatus;

determining whether transmitting said portion of said controlled item to said second apparatus is authorized based at least in part on said second apparatus information; and

if transmission is authorized, transmitting said portion from said first apparatus to said second apparatus.

15. A method as in claim 14, in which said second apparatus information includes information relating to the level of security, integrity, or copy protection present at said second apparatus.

16. A method including:

at a first apparatus, receiving a first secure digital container including a controlled item, said controlled item including a file and information steganographically encoded into said file, said information including a first control set made up of at least one control;

at said first apparatus, retrieving at least a portion of said controlled item from said first secure digital container;

at said first apparatus, steganographically recovering said first control set from said controlled item; and

at said first apparatus, using said first control set to control at least one aspect of access to or use of at least a portion of said controlled item, including directly or indirectly providing payment-related information to a second apparatus.

17. An apparatus including the following elements:

a portable memory reader;

a processing unit;  
a memory; and  
a portable memory including:  
a first secure digital container,  
a controlled item and information steganographically encoded in said controlled item; and  
control information relating to at least one aspect of control of said controlled item, including a control based at least in part based on information relating to the age of a user of said apparatus.

18. An apparatus including the following elements:

a portable memory reader;  
a processing unit;  
a memory; and  
a portable memory including:  
a first secure digital container,  
a controlled item and information steganographically encoded in said controlled item; and  
control information including at least one control at least in part controlling when at least a portion of said item is capable of being converted from a first format to a second format and of being stored in said second format.

19. An apparatus as in claim 18, in which said first format comprises a digital format and said second format comprises an analog format.

20. An apparatus as in claim 18, in which said first format comprises an analog format and said second format comprises a digital format.

21. A secure digital container including:

an encrypted controlled item comprising digital information;  
first control information steganographically encoded into said controlled item;  
second control information;  
said first or second control information including information relating to the age of a user; and  
a cryptographic key capable of being used to at least in part decrypt said controlled item.

22. A secure digital container including:

an encrypted controlled item comprising digital information;  
first control information steganographically encoded into said controlled item;  
second control information;  
said first or second control information including at least one control at least in part controlling whether at least a portion of said item is capable of being converted from a first format to a second format and of being stored in said second format; and

a cryptographic key capable of being used to at least in part decrypt said controlled item.

23. A secure digital container as in claim 22, in which said first format comprises a digital format and said second format comprises an analog format.

24. A secure digital container as in claim 22, in which said first format comprises an analog format and said second format comprises a digital format.

25. A secure digital container including:

encrypted controlled contents comprising digital information;

a first digital control of a first entity, said first digital control controlling at least one aspect of access to or use of at least a portion of said controlled contents;

a second digital control of a second entity different from said first entity, said second digital control controlling at least one aspect of access to or use of at least a portion of said controlled contents;

said first or second digital controls including at least one control based at least in part on information relating to the age of a user; and

information steganographically encoded in said controlled contents.

26. A secure digital container including:

encrypted controlled contents comprising digital information;

a first digital control of a first entity, said first digital control controlling at least one aspect of access to or use of at least a portion of said controlled contents;

a second digital control of a second entity different from said first entity, said second digital control controlling at least one aspect of access to or use of at least a portion of said controlled contents;

said first or second digital controls including at least one control at least in part controlling whether at least a portion of said item is capable of being converted from a first format to a second format and of being stored in said second format; and

information steganographically encoded in said controlled contents.

27. A secure digital container as in claim 26, in which said first format comprises a digital format and said second format comprises an analog format.

28. A secure digital container as in claim 26, in which said first format comprises an analog format and said second format comprises a digital format.

29. A secure digital container including:

a controlled item comprising digital information, said controlled item being at least in part encrypted;

a first control steganographically encoded into at least a portion of said controlled item, said first control controlling at least one aspect of access to or use of at least a portion of said controlled item;

a second control controlling at least one aspect of access to or use of at least a portion of said controlled item; said second control being different from said first control;

said first or second controls including at least one control based at least in part on information relating to the age of a user of said apparatus.

30. A secure digital container including:

a controlled item comprising digital information, said controlled item being at least in part encrypted;

a first control steganographically encoded into at least a portion said controlled item, said first control controlling at least one aspect of access to or use of at least a portion of said controlled item;

a second control controlling at least one aspect of access to or use of at least a portion of said controlled item; said second control being different from said first control

said first or second controls including at least one control at least in part controlling whether at least a portion of said item is capable of being converted from a first format to a second format and of being stored in said second format.

31. A secure digital container as in claim 30, in which said first format comprises a digital format and said second format comprises an analog format.

32. A secure digital container as in claim 30, in which said first format comprises an analog format and said second format comprises a digital format.